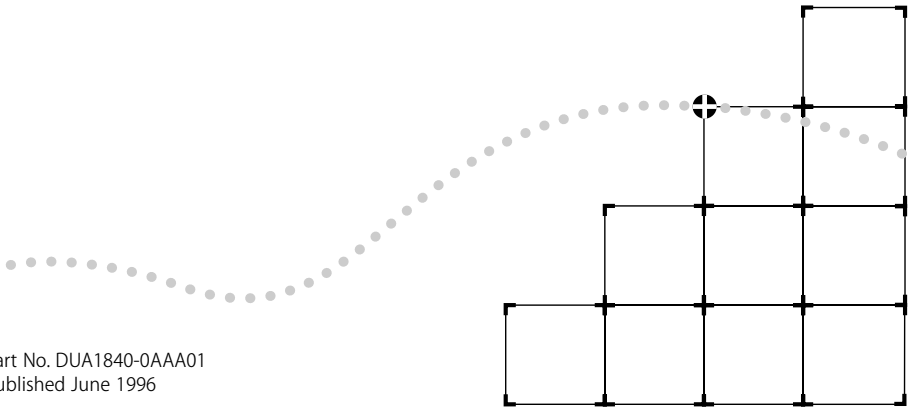
MSH Switch 1005
User Guide



Part No. DUA1840-0AAA01
Published June 1996

3Com Corporation ■ 5400 Bayfront Plaza ■ Santa Clara, California ■ 95052-8145

3Com Ireland reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Ireland to provide notification of such revision or change.

3Com Ireland provides this documentation without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

UNITED STATES GOVERNMENT LEGENDS:
If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following restricted rights:

For units of the Department of Defense:
Restricted Rights Legend: Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) for restricted Rights in Technical Data and Computer Software clause at 48 C.F.R. 52.227-7013. 3Com Ireland, c/o Isolan House, Brindley Way, London Road, Hemel Hempstead, Herts., HP3 9XJ, United Kingdom.

For civilian agencies:
Restricted Rights Legend: Use, reproduction or disclosure is subject to restrictions set forth in subparagraph (a) through (d) of the Commercial Computer Software - Restricted Rights Clause at 48 C.F.R. 52.227-19 and the limitations set forth in 3Com Corporation's standard commercial agreement for the software. Unpublished rights reserved under the copyright laws of the United States.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, LinkBuilder and Transcend are registered trademarks of 3Com Corporation. SuperStack II, PACE, VLT, Virtual LAN Trunk and 3TECH are trademarks of 3Com Corporation. 3ComFacts is a service mark of 3Com Corporation.

CompuServe is a registered trademark of CompuServe, Inc..

Other brand and product names may be registered trademarks or trademarks of their respective holders.

CONTENTS

2 INSTALLATION AND INITIAL SETUP

3 SWITCH CONFIGURATION

4 ADVANCED MANAGEMENT

5 STATUS MONITORING AND STATISTICS

6 PROBLEM SOLVING

About This Guide

Introduction

This guide describes how to install and configure the MSH Switch 1005.

If the information in the release notes shipped with your product differs from the information in this guide, follow the release notes.

How to Use This Guide

The following table shows where to find specific information in this guide.

If you are looking for:	Turn to:
A description of all the Switch 1005 features and a guide to making a quick start with management	Chapter 1
Important safety information, a brief overview of the installation process and a complete guide the initial setup required	Chapter 2
Information and steps telling you how you can manage the Switch 1005 using the VT100 screens	Chapter 3
Information on the more advanced functionality you can manage using the VT100 screens	Chapter 4
Details on viewing Switch 1005 statistics using the VT100 screens	Chapter 5
Ideas on solving problems should they arise	Chapter 6
A list of user access rights for the VT100 screens	Appendix A
Technical information about the Switch 1005	Appendix B
Technical support information	Appendix C
A list of terms and definitions used in this Guide	Glossary
A comprehensive Index	Index

Conventions

Table 1 and Table 2 list text and icon conventions that are used throughout this guide:

Table 1 Notice Icons

Icon	Type	Description
	Information Note	Information notes call attention to important features or instructions.
	Caution	Cautions alert you to personal safety risk, system damage, or loss of data.
	Warning	Warnings alert you to the risk of severe personal injury.

Table 2 Text Conventions

Convention	Description
"Enter" vs. "Type"	When the word "enter" is used in this guide, it means type something, then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."
Text represented as `screen display`	`This typeface` is used to represent displays that appear on your terminal screen, for example: `NetLogin:`
Text represented as **`commands`**	**`This typeface`** is used to represent commands that you enter, for example: **`SETDefault !0 -IP NETaddr = 0.0.0.0`**
Keys	When specific keys are referred to in the text, they are called out by their labels, such as "the Return key" or "the Escape key," or they may be shown as [Return] or [Esc]. If two or more keys are to be pressed simultaneously, the keys are linked with a plus sign (+), for example: Press [Ctrl]+[Alt]+[Del].
Italics	Italics are used to denote new terms or emphasis.

Related Publications

This User Guide is not intended to answer all your questions concerning the MSH. While using the MSH Switch 1005, you may need to refer to the following publications:

- *LinkBuilder MSH User Guide*, part number DUA1800-0AAA0x.
- *LinkBuilder MSH Management Module User Guide*, part number DUA1850-0AAA0x.

1 GETTING STARTED

About the LinkBuilder MSH

The LinkBuilder MSH is an extremely versatile, chassis-based hub that allows you to connect and manage large, mixed-technology, mixed-media LANs.

The basis of the MSH is the chassis into which you can install a series of network-specific modules. Modules within the chassis connect to a number of backplanes allowing communication between the various LANs and LAN segments connected to the MSH.

About the MSH Switch 1005

The MSH Switch 1005 is designed to be installed into the MSH chassis, so that you can extend your network beyond the limits of a repeater and provide your users with greater bandwidth, faster throughput, and high speed connections.

The MSH Switch 1005 is an intelligent module with its own on-board management agent. This means that even in an unmanaged MSH chassis, you can access the manageable features of the Switch using a Telnet application or an SNMP Network Manager and configure internal port connections using the five links located on the Switch.

With a Management Module installed into your MSH chassis, you have access to the VT100 interface of the Switch. This interface provides a series of ASCII character-based forms which allow you to configure the manageable features of the Switch. You can find further information about Switch management in "Setting up the Switch 1005" in Chapter 2.

Summary of Features

- 8 switched 10BASE-T ports
- Slot for optional Fast Ethernet or 10BASE-T Transceiver Module
- Switched connections to all 3 internal Ethernet backplanes
- Internal Fast Ethernet backplane
- Ability to add Expansion Module adding up to three further Transceiver Modules
- Support for up to 500 end-stations, unlimited stations on backbone port
- Forwarding modes for packets
  - Low latency in fast forward mode
  - No runts in fragment free mode
  - No runts/errors in store-and-forward mode
  - Low latency or no runts/errors in intelligent mode
- Intelligent Flow Management when packet buffers are full
  - Prevents packets being discarded
  - Suppresses transmissions at source
- Full duplex on Fast Ethernet Transceiver Modules
- Security
- Resilient Links
- Port-based Virtual LANs (VLANs)
  - Support for up to 16 VLANs on a single Switch 1005
  - Eases the movement of devices on IP networks
  - Controls traffic
  - Provides extra security
- PACE (Priority Access Control Enabled)
  - Supports multimedia applications over Ethernet
  - Increased Ethernet predictability
  - Full use of network bandwidth

- SmartAgent support
  - SNMP with IP and IPX protocols
  - RMON
  - Repeater and Bridge MIB
  - Broadcast storm control
  - Easy software upgrades
  - BOOTP
  - Local management

Port Connections

10BASE-T Switch Ports

Eight fixed ports each configured as MDIX provide 10Mbps bandwidth to each attached end-station. Maximum segment length is 100m (328ft) over grade 3, 4 or 5 twisted pair cable.

Internal Switch Ports

As well as switch ports located on the front panel of the Switch 1005, internal backplane connections provide an additional four switch ports. These ports are enabled and disabled through management or using the set of links LK1 to LK5 located on the Switch 1005.

Three of these ports provide switched connections to the three 10Mbps repeater backplanes located in the MSH chassis, and therefore to any modules connected to the same backplane.

The fourth internal switched port provides a connection to the Fast Ethernet backplane, and therefore to any other Switch 1005 modules installed in the chassis.

Locating and setting links is described in "Setting the Links on the Switch 1005" in Chapter 2.

Transceiver Module Ports

A slot on the front of the Switch 1005 allows you to install any of the Transceiver Modules available for this product. You can find more details in "Transceiver Module slot" on page 1-18.

The Backbone Port

The MSH Switch 1005 requires that the port connecting it to the rest of your network is configured as a *backbone port*. This is the port to which all frames arriving at a switch port with an unknown destination address will be forwarded. Addresses received on the backbone port are not stored in the switch database of the Switch 1005.

When you first install a Switch 1005 into your MSH chassis, it will configure its backbone port to be the first Fast Ethernet port it finds either on the Switch, or on the Expansion Module if fitted. You can change your designated backbone port to be any switch port (internal or external). Changing the default backbone port is described in "Specifying the Backbone Port" in Chapter 3.

You can only have one backbone port per Switch 1005, unless you have implemented multiple VLANs on one Switch; in this case you can configure one backbone port per VLAN. You can find more information about VLANs in Chapter 4.

Adding an Expansion Module

The MSH Switch 1005 also has provision for installing an Expansion Module. The Expansion Module has three slots for installing any combination of the Transceiver Modules described in "Transceiver Module slot" on page 1-18.

Switch Operation and Features

How the Switch Compares to a Bridge

The table below shows how Switch 1005 operation compares to that of an IEEE 802.1D bridge:

	IEEE 802.1D Bridge	Switch 1005
Address Learning	All ports	All ports except backbone.
Forwarding Mode	Store-and-forward	Fast Forward, Fragment Free, Store and Forward, or Intelligent
Operation when packet buffers full	Discard packets	Invoke Intelligent Flow Management to suppress transmissions at source
Spanning Tree	Supported	Not supported
Action on Unknown Destination Address	Flood all ports	Forward to backbone port only
Database size	Variable	500 addresses

In all other ways, MSH Switch 1005 and bridge operation is identical.

Forwarding of Packets

The table below shows how a packet is processed when it arrives at the Switch 1005:

Packet Source	Destination Address	Action
Any port EXCEPT backbone port (Unicast packet)	Unknown	Forward to backbone port only
Any port EXCEPT backbone port (Unicast packet)	Same port as source address	Filter (discard)
Any port EXCEPT backbone port (Unicast packet)	Another port (not backbone port)	Forward to specific port only

Packet Source	Destination Address	Action
Any port EXCEPT backbone port (Multi/Broadcast packet)	Not applicable	Forward to all ports (including backbone port) within same VLAN as source port
Backbone port (Unicast packet)	Unknown	Filter (discard)
Backbone port (Unicast packet)	Known on a port (not backbone port)	Forward to specific port only
Backbone port (Multi/Broadcast packet)	Not applicable	Forward to all ports within specific VLAN

To best suit your networking requirements, the Switch 1005 allows you to set one of four frame forwarding modes:

- **Fast Forward** — In this mode, frames are forwarded as soon as the destination address is received and verified. The forwarding delay, or latency, for all frames in this mode is just 40µs but with the lack of checking time, any collision fragments or error frames received are propagated through the switch.
- **Fragment Free** — In this mode, a minimum of 64 bytes of the received frame is buffered prior to the frame being forwarded. This ensures that collision fragments are not propagated through the network, however, CRC errors are forwarded. The forwarding delay, or latency, for all frames in this mode is 64µs.
- **Store and Forward** — In this mode, received packets are buffered in their entirety prior to forwarding. This ensures that only good frames are passed to their destination. The forwarding delay for this mode varies between 64µs and 1.2ms, depending on frame length. In Store and Forward mode, latency is measured as the time between receiving the last bit of the frame, and transmitting the first bit. For the Switch 1005, this is 8µs.
- **Intelligent** — In this mode, the Switch 1005 monitors the amount of error traffic on the network and changes the forwarding mode accordingly. If the Switch 1005 detects less than 18 packets per second with errors, it will operate in Fast Forward mode. As soon as the Switch 1005 detects more than 18 packets per second with errors, it will operate in Store and Forward mode until the error count returns to 0.

Intelligent Flow Management

Intelligent Flow Management (IFM) is a congestion control mechanism built into the Switch 1005. Congestion is caused by one or more devices sending traffic to a Switch port which is already busy. The Switch 1005 contains both input and output packet buffers and while congestion is rare, IFM is designed to alleviate problems during those moments when packet buffers in the Switch 1005 are full. IFM will prevent packet loss by inhibiting the transmitting device from sending any further packets until the port is no longer congested.

If a packet arrives at a conventional switch that does not operate IFM, and that port is congested, the transmitting device is unaware of this until it times out and decides that the receiving station is not going to respond to the message. This can take as long as 30 seconds, and depending on the protocol you are running, may not happen until many packets have been sent. The transmitting device then has to retransmit the packets, effectively wasting bandwidth.

Switch modules implementing IFM are aware of congestion, and prevent packet loss by inhibiting the transmitting device from transmitting the packet in the first place. It does this by forcing the device to retransmit the packet later. This "back-off" and retransmission happens very quickly (typically less than one second) and is much faster than waiting for the transmitting device to time-out. There are two benefits:

- the packet is transmitted quickly and successfully
- the packet is only transmitted once, thereby saving bandwidth.

IFM is designed to be enabled on ports connected to a single network device. If IFM is enabled on a port connected to multiple devices through a repeater, packet congestion within the Switch 1005 could result in packet transmission between two devices connected to the repeater being inhibited.

Full Duplex

The MSH Switch 1005 provides full duplex support for any Fast Ethernet Transceiver Modules you may have installed. Full duplex allows frames to be transmitted and received simultaneously and, in effect, doubles the bandwidth available on the link. Full duplex also supports 100BASE-FX cable runs of up to 2km.

Security

The MSH Switch 1005 contains advanced security features which guard against users connecting unauthorized stations onto your network. When security is enabled on a port, that port enters into a single address learning mode. This port is then permitted to learn just a single Ethernet address and once this is learned, if a different address is then seen on that port, the port will be disabled. Until security is disabled, no other address can be learned.

Resilient Links

The Resilient Link feature in the Switch 1005 enables you to protect critical links and prevent wasteful network downtime should that link fail. Setting up resilience ensures that should a main communication link fail, a standby duplicate link will immediately and automatically take over the task of the main link. Each main and standby link pair is referred to as a resilient link pair. The main and standby links must be set up on the same Switch 1005.

Virtual LANs (VLANs)

The Switch 1005 has a Virtual LAN (VLAN) feature which allows you to build your network segments without being restricted by physical connections. A VLAN is defined as a group of location- and topology-independent devices that communicate as if they are on the same physical LAN.

Implementing VLANs on your network has three main advantages:

- Network administration personnel are required to make less physical intervention when a workstation has to be moved. Within the VLAN setup, a group of devices on different floors in a building can be configured into a common communications group. If a workstation is moved from VLAN 1 to VLAN 2 for example, the network administrator only needs to know address information for that device; the physical location of the port is irrelevant.
- Use of network resources becomes much more efficient. Each VLAN can be set up to contain only those devices which need to communicate with each other. In this way, broadcast storms, the most common cause of network congestion, can also be avoided.
- Network security is enhanced. Devices within each VLAN can only communicate with member devices in the same VLAN. If a device in VLAN 1 for example, needs to communicate with devices in VLAN 2, it must be configured to cross the router between them.

Further information can be found in Chapter 4.

PACE

PACE (Priority Access Control Enabled) technology allows multimedia applications using voice and video traffic to be carried over standard Ethernet and Fast Ethernet Local Area Networks (LANs). PACE provides the quality of service that these applications require, reducing latency to a minimum and prioritizing the multimedia traffic.

Both multimedia and data traffic are improved considerably by introducing an Ethernet switch into the LAN and attaching each end-station to its own dedicated 10Mbps switch port. This removes any contention between different end-stations for the Ethernet bandwidth. However, when two-way traffic is passing between an end-station and the switch port, access to the bandwidth can still be unfairly allocated to traffic in one direction, resulting in poor quality video display. PACE allocates the available bandwidth fairly to traffic in each direction. In this way, existing Ethernet adapters and cabling can be used to run high-quality multimedia sessions across the LAN.

You can enable PACE on the whole Switch 1005 module or on an individual port. Before configuring PACE, you should refer to sections "Switch 1005 Setup" and "Port Setup" in Chapter 3.

MSH Switch 1005 on Your Network

Server Connections

When integrating the Switch 1005 into your network, the following notes on server connections will ensure that it is operating at maximum efficiency:

- Ideally ...

  ... any local server should be connected to the Switch 1005 using a 100Mbps port.

- If that is not possible ...

  ... connect the local server to a dedicated 10Mbps port.

- If that's not possible and the local server is connected to a repeated segment where the traffic is mainly local to that segment ...

  ... disable Intelligent Flow Management (IFM) on the port to which the repeater is connected.

Whenever you have multiple workstations connected to a single port of the Switch 1005, we recommend that you disable IFM on that port.

Network Configuration Examples

The following illustrations show some examples of how the Switch 1005 can be used on your network.

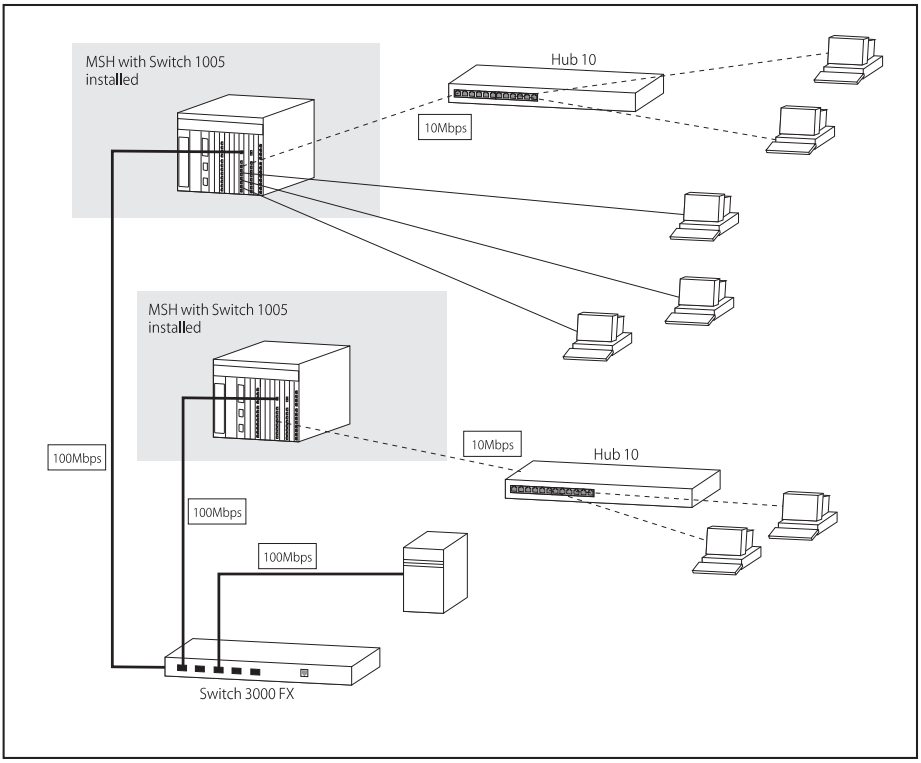


Figure 1-1 Workgroup Switch I

Figure 1-1 shows how the Switch 1005 fits into a large corporate network with a Fast Ethernet infrastructure. A Switch is positioned on each floor and servers are centralized in the basement.

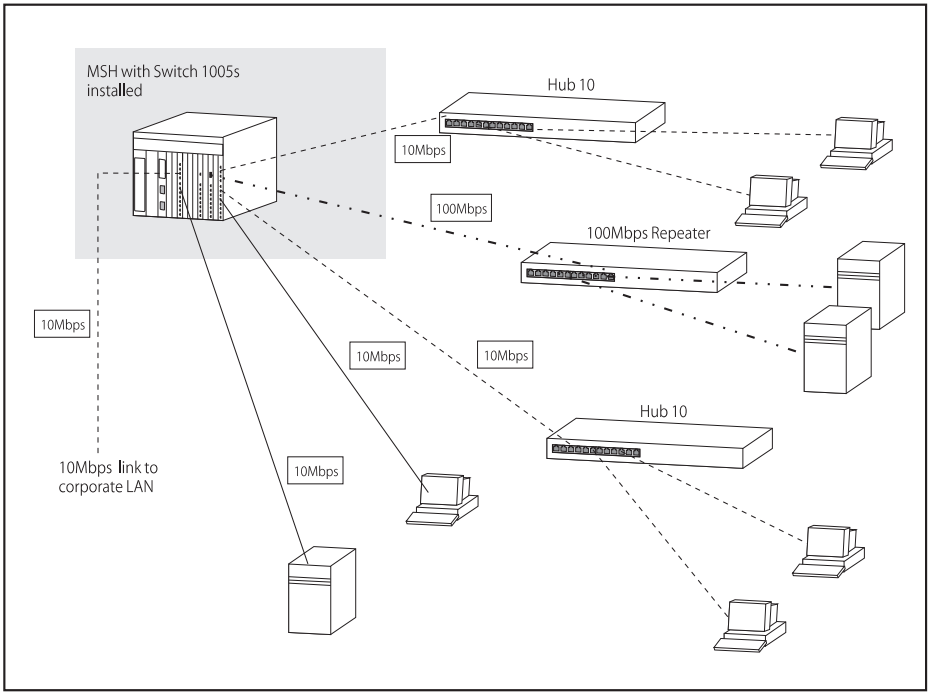


Figure 1-2 Workgroup Switch II

Figure 1-2 shows the Switch 1005 in a second workgroup situation. This setup could be that of a small office within a large corporation, or part of a larger corporate network. Each switch port has mainly muliple end-stations.

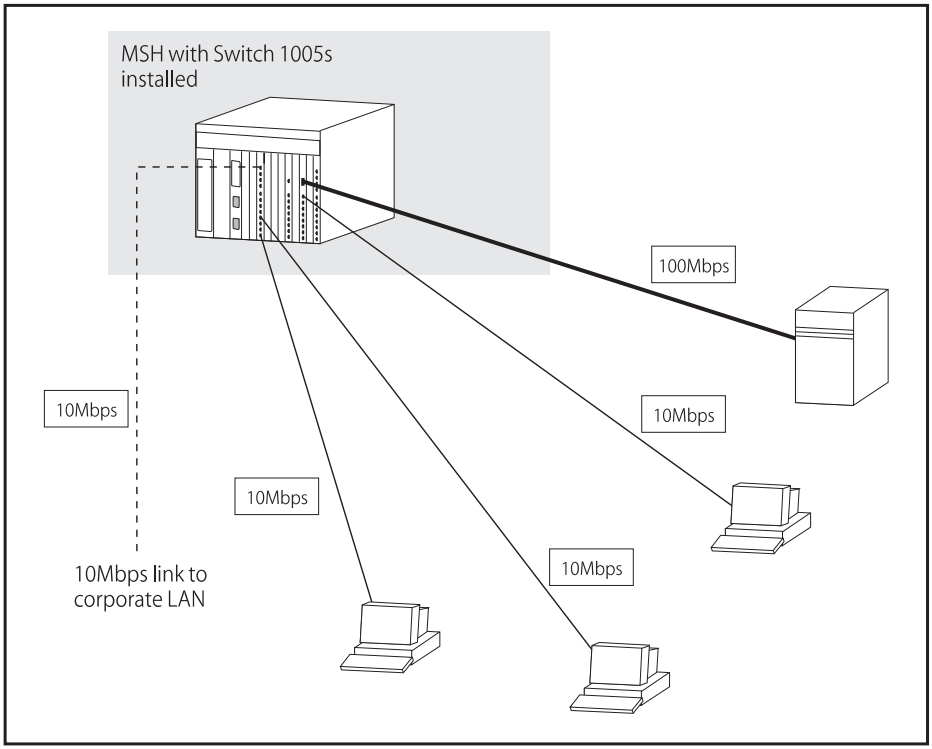


Figure 1-3 Desktop Switch

Figure 1-3 shows the Switch 1005 used for a group of heavy-traffic users in a large corporate network. Here, switching is brought to the desktop with a single end-station per switch port. Local servers are connected via a 100Mbps Fast Ethernet link.

Configuration Rules for Fast Ethernet

The topology rules for Fast Ethernet (100Mbps) are slightly different to those for 10Mbps Ethernet. The key topology rules are:

- Maximum UTP cable length is 100m (328ft) over *category 5* cable.
- A 412m (1352ft) fiber run is allowed for connecting switch to switch, or end-station to switch, using standards-compliant half-duplex 100BASE-FX.
- A total network span of 325m (1066ft) is allowed in single-repeater topologies (one hub stack per wiring closet with a fiber run to the collapsed backbone); for example, a 225m (738ft) fiber downlink from a repeater to a router or switch, plus 100m (328ft) UTP run from a repeater out to the desktops.

Configuration Rules with Full Duplex

The MSH Switch 1005 provides full duplex support for any Fast Ethernet Transceiver Modules that are installed. Full duplex allows frames to be transmitted and received simultaneously and, in effect, doubles the bandwidth available on a link.

With full duplex, the topology rules are:

- Maximum UTP cable length is still 100m (328ft) over *category 5* cable.
- A 2km (6562ft) fiber run is allowed for connecting switch to switch, or end-station to switch.

Switch Overview — Front Panel

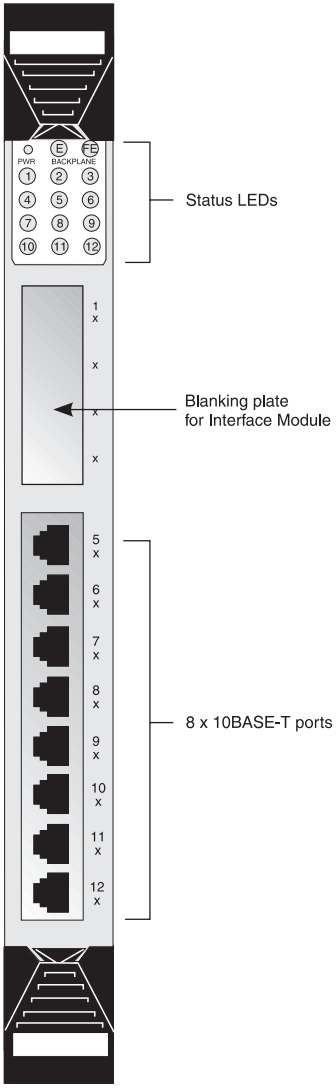


Figure 1-4 Switch 1005 front view

LEDs

LED	Color	Indicates ...
PWR (Power)	Green	The Switch is powered up and operating normally.
	Green flash (slow, 0.5 Hz)	Power On Self Test (POST) in operation.
	Green flash (fast, 1Hz)	Software download in progress
	Amber	Fault occurred on this Switch
Backplane E	Green	One or more of the internal Ethernet (10Mbps) backplanes are enabled.
	Green flash	All three internal Ethernet backplanes are disabled.
	Yellow	There is network activity on the enabled backplane(s).
FE	Green	Connection to the internal Fast Ethernet (100Mbps) backplane is enabled.
	Green flash	Connection to the internal Fast Ethernet (100Mbps) backplane is disabled.
	Yellow	There is network activity on the Fast Ethernet backplane.
1 - 12 (External port status)	Green	Link connected; port enabled.
	Green flash	Link connected; port disabled.
	Yellow	Traffic being transmitted/received on this port.
	Off	Link not connected.
	Ports 1 - 4 relate to any Transceiver Module installed into the slot. If you have installed a Fast Ethernet Transceiver Module, LED 1 will be lit, all others are unused.	

For information on using the LEDs for fault diagnosis, please see "Identifying Fault Conditions with the LEDs" in Chapter 6.

Transceiver Module slot

Allows you to install an Transceiver Module. Transceivers available include:

- **100BASE-TX Transceiver Module (3C18407)** — This Fast Ethernet, 100Mbps, twisted pair port provides the Switch with a single, high-speed connection to, for example, your network infrastructure. Maximum segment length is 100m (328ft) over grade 5 twisted pair cable.
- **100BASE-FX Transceiver Module (3C18408)** — This Fast Ethernet, 100Mbps, fiber port provides the Switch with a single, high-speed connection to, for example, your network infrastructure. Use 62.5/125 micron fiber optic cable with SC connectors. The maximum supported distance is 412m (1352ft) or 2km (6562ft) if the devices at both ends of the link support full duplex.
- **4 Port 10BASE-T Transceiver Module (3C18409)** — Adds an additional four 10BASE-T ports to your Switch 1005 with the same operating conditions as the eight fixed ports described below.

You should contact your supplier for further details on these and any further Transceiver Modules available from 3Com.

10BASE-T Ports

Eight fixed ports each configured as MDIX provide the full 10Mbps bandwidth to each attached end-station. Maximum segment length is 100m (328ft) over grade 3, 4 or 5 twisted pair cable.

Switch Overview — PCB View

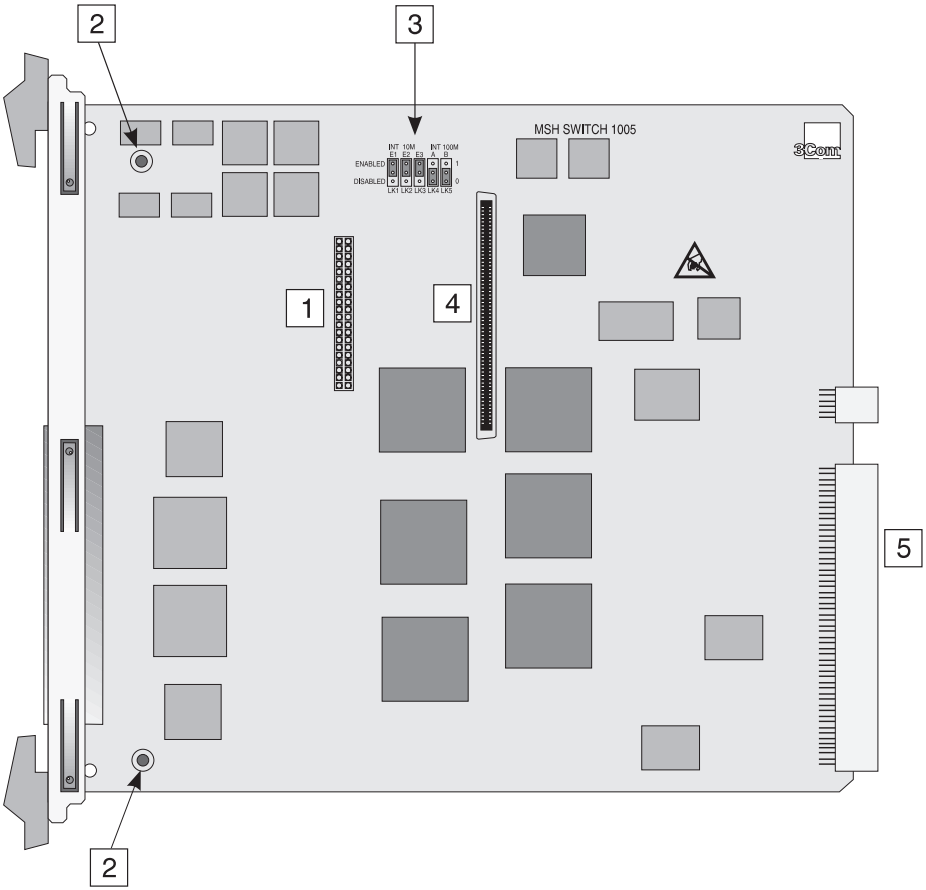


Figure 1-5 Switch 1005 PCB view

Transceiver Module Connector [1]

2x20 pin connector for any of the Transceiver Modules listed in "Transceiver Module slot" on page 1-18. Installation of the Transceiver Modules is described in the documentation that accompanies them.

Expansion Module Fixing Posts [2]

The two threaded posts provide fixing points for an Expansion Module should you choose to attach one to this Switch.

Links LK 1 to LK 5 [3]

Allow you to configure internal backplane connections for the Switch 1005. See "Setting the Links on the Switch 1005" in Chapter 2.

Expansion Module Socket [4]

This socket provides the connection point for an Expansion Module should you choose to fit one to this Switch.

Backplane Connectors [5]

These connectors engage with the backplane located in the MSH chassis.

Switch Defaults

The following table shows factory defaults for the MSH Switch 1005:

Port Status	Enabled
Forwarding Mode	Fast Forward
Intelligent Flow Management (IFM)	Enabled on external ports Disabled on internal ports
PACE	Disabled (module)
VLANs	All ports in the Default VLAN (VLAN 1)
Power On Self Test (POST)	Normal
RMON	1 Ethernet Statistics session per port/VLAN.
	3 Stats History sessions on the backbone port and 3 on the Default VLAN
	1 Host Table session on the Default VLAN
	4 Matrix Table sessions; 1 on the Default VLAN, 1 on port 25, 1 on port 26 and 1 on port 27
	4 default alarms per port
	Default events for use with the alarm system

Setting Up the MSH Switch 1005 for Management

This section describes how to get started if you wish to use an SNMP manager. It assumes you are already familiar with SNMP management.

- If you are using IP and you have a BOOTP server setup correctly on your network, the IP address for the Switch 1005 will be detected automatically and you can start managing the Switch 1005 without any further configuration.
- If you are using the IPX protocol, the Switch 1005 will be allocated an IPX address automatically. You can start the SNMP Network Manager and begin managing the Switch 1005.
- If you are using IP without a BOOTP server, you will need to enter the IP address of the Switch 1005 before the SNMP Network Manager can communicate with the device. To do this, perform the following steps:

1 Ensure your MSH Management Module is running v4.2 or higher of the management agent software.

2 Connect a terminal to the serial port located on the MSH front panel. You can find instructions for doing this in the *LinkBuilder MSH Management Module User Guide*, part number DUA1850-0AAA0x.

3 Press [Return] one or more times until the MSH Main Banner appears. The serial port will detect the terminal line speed (baud rate) and default to:

- 8 data bits
- 1 stop bit
- no parity

You cannot modify these settings. If your terminal is already setup with these values, the MSH Main Banner will appear as soon as power-up is complete. Press [Return] to display the MSH Main Menu.

4 At the MSH Main Menu, select SERVICE SELECTION. From the Service Selection list, select Switch 1005. From the Address Table screen, choose the required Switch 1005 and select MANAGE. The Switch Main Banner screen appears.

5 At the Switch 1005 Main Banner, press [Return] to display the Logon screen. Logon using the default name *security*, and password *security*. Select OK.

6 The Switch Main Menu is displayed. From this menu, select the Management Setup option. The Switch Management Setup screen is displayed.

7 On the Management Setup screen, fill in the following fields:

- Device IP Address
- Device SubNet Mask (if necessary)
- Default Router (if necessary)

For further information on the Management Setup screen, see "Switch 1005 Management Setup" in Chapter 2.

8 If you need the Switch to send SNMP traps to the network manager, you may need to setup the address of the network manager in the Trap Table. See "Setting Up Traps" in Chapter 3.

3Com Network Managers such as Transcend WorkGroup Manager for Windows may automatically configure intelligent modules to send traps to them. Please read the documentation supplied with your network management software.

9 When you have finished with the Management Setup screen, select OK.

Once the module's IP parameters are specified, you can continue management using:

- In-band management via any SNMP-based Network Manager application.
- Out-of-band management via the Switch 1005's own VT100 management interface.
- In-band management via the Switch 1005's own VT100 management interface.

2 Installation and Initial Setup

Safety Information

Before installing the MSH Switch 1005 into your MSH chassis, you should consider the following safety information:

- Installation and removal of the Switch 1005 should be carried out by qualified personnel only.
- The Switch 1005 operates under SELV conditions (Safety Extra Low Voltage) according to IEC 950, the conditions of which are met only if the equipment to which it is connected is also operational under SELV.
- The MSH chassis must be earthed.
- Switch 1005 modules can easily be damaged by static:
  - Do not remove the Switch 1005 from its anti-static packaging until you are ready to install it into the MSH chassis.
  - Do not touch the pins, leads, connections or any components on the Switch 1005.
  - Always handle the Switch 1005 by its edges only.
  - Always wear an anti-static wristband connected to a suitable earth point.
  - Always store and transport the Switch 1005 in anti-static packaging.
- The MSH chassis can be powered up during Switch 1005 installation.

Pre-installation Configuration

Before installing the Switch 1005 into the chassis, ensure it is configured to suit your particular requirements. Procedures that must be carried out prior to installation include:

- Setting links located on the Switch 1005.
- Fitting a Transceiver Module if required.
- Fitting an Expansion Module if required.

Setting the Links on the Switch 1005

Five links located on the Switch 1005 allow you to set up its backplane connections.

The links are located on the Switch 1005 PCB as shown in Figure 2-1.

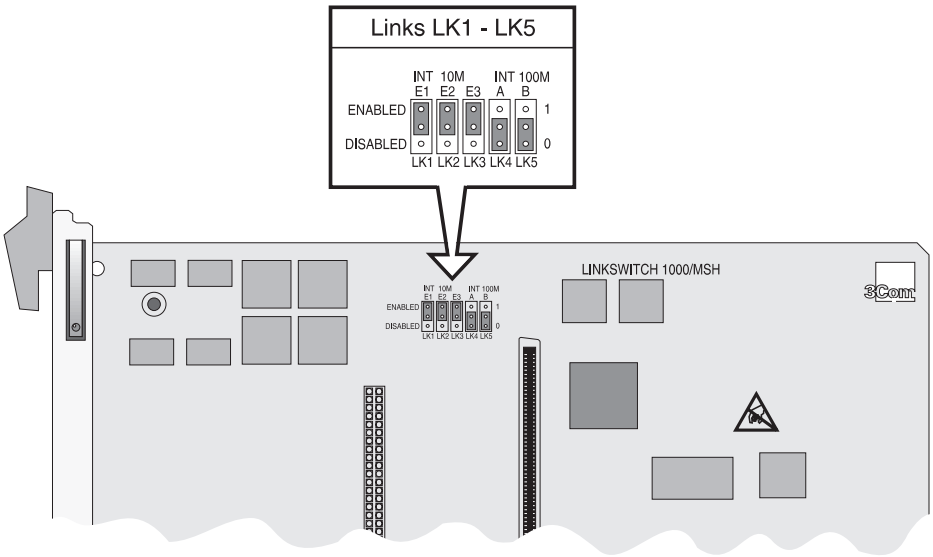
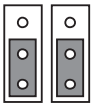
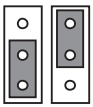
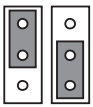
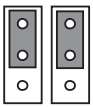


Figure 2-1 Locating links LK1, LK2, LK3, LK4, LK5

Table 2-1 shows possible configurations for LK1 - LK5. You may have any combination of backplane connections enabled at any one time.

In a managed MSH chassis, these links will be overridden by any changes made through management software. This is the case, even if the chassis is reset or powered off/on, or if the Switch 1005 module is replaced with another one.

Table 2-1 Setting LK1 - LK5 for internal port connections

	Position and Link Number	Connection Provided
	LK1 ENABLED	Switch port 25 connected to 10Mbps Ethernet backplane E1.
	LK2 ENABLED	Switch port 26 connected to 10Mbps Ethernet backplane E2.
	LK3 ENABLED	Switch port 27 connected to 10Mbps Ethernet backplane E3.
	LK1, LK2, LK3 DISABLED	None
	LK4 DISABLED, LK5 DISABLED	Switch port 28 disabled
	LK4 DISABLED, LK5 ENABLED	Switch port 28 connected to 100Mbps Fast Ethernet backplane. This allows you to interconnect multiple Switch 1005 modules.
	LK4 ENABLED, LK5 DISABLED	Reserved for future use.
	LK4 ENABLED, LK5 ENABLED	Reserved for future use.

Advice for Setting Backplane Connections and Avoiding Loops

Considerable care should be taken when setting backplane connections if there is more than one Switch 1005 installed in your MSH chassis. If more than one module has multiple connections enabled on the same VLAN, a network loop can occur, severely affecting network operation.

For example, consider a pair of Switch modules where all four backplane connections are enabled and in the same VLAN. If a packet with a unicast destination address arrives on the backplane E1, destined for an end-station on backplane E2, both Switch modules will independently switch the packet onto E2, resulting in duplication. Packets with broadcast destination addresses will loop continuously between the two Switch modules. You can avoid this situation by following these guidelines:

- If all ports on your network are in the same VLAN, you should connect all Switch 1005 modules via the Fast Ethernet connection, but only connect the internal Ethernet backplanes on one Switch 1005.
- Alternatively, balance the load on your Switch 1005 modules more effectively by connecting one internal Ethernet connection to each Switch 1005.
- If you have implemented multiple VLANs, put each internal Ethernet connection in a different VLAN on each Switch.

Fitting a Transceiver Module

The MSH Switch 1005 has a slot for one Transceiver Module. You should fit the Transceiver Module before you fit the Expansion Module and before you install the Switch 1005 into the MSH chassis. Fitting the Transceiver Module is described in the User Guide that accompanies it.

If you have an Expansion Module fitted to your Switch 1005 and you install four 4 Port 10BASE-T Transceiver Modules with all backplane connections enabled, Ethernet backplane E3 (port 27) will automatically disable and you will lose the ability to configure it. Removing one of the Transceiver Modules will reinstate port 27.

Fitting an Expansion Module

Fitting an Expansion Module allows you to increase the number of ports for your Switch 1005; you should fit it to the Switch 1005 before installing the pair into the MSH chassis. The Expansion Module provides three locations for Transceiver Modules. You should fit these before you fit the Expansion Module. Fitting the Expansion Module is described in the User Guide that accompanies it.

Switch 1005 Installation and Removal

The following steps give a brief guide to installing the Switch 1005 into the chassis and removing it. For detailed instructions, refer to the *LinkBuilder MSH User Guide*, part number DUA1800-0AAA0x.

Installing the Switch 1005

1 If you have a Management Module installed, ensure that both the MSH chassis and the Management Module are powered on.

If you do not have a Management Module installed, the Switch 1005 can be installed whether the MSH chassis is powered on or off.

2 Undo the screws from the locking bar of the MSH chassis and lift the bar away from the chassis.

3 Undo the screws from the blanking plate of the slot of your choice. Keep the blanking plate in a safe place. If you remove the Switch 1005, you must cover any open slot with a blanking plate to maintain the circulation of cooling air and prevent the entry of dust and debris into the MSH.

4 Holding the Switch 1005 by the front panel, insert it into the guides and push in fully.

5 Operate the ejectors to secure the Switch 1005.

6 Replace the locking bar and secure it with the screws you removed earlier.

Once it is correctly installed in the MSH chassis and the chassis is powered up, the Switch 1005 will run through its Power On Self Test (POST) sequence. The LEDs on the front panel will flash during the POST; see "LEDs" in Chapter 1 for more information.

Removing the Switch 1005

You do not need to power off the MSH chassis before removing the Switch 1005. However, you should warn any users attached to the Switch of the disruption in operation.

1 Undo the screws from the locking bar of the MSH chassis and lift the bar away from the chassis.

2 Operate the module ejectors correctly, as shown in the MSH User Guide referenced above. Store the removed Switch safely to avoid damage. Note that the ejectors on the Expansion Module are dummy.

3 If you are not going to install a replacement module in the vacated slot immediately, cover with a blanking plate.

4 Replace the locking bar and secure with the screws removed earlier.

Operation after Power-up

In an Unmanaged System

The links LK1 to LK5 are used to set the Switch's backplane connections in an unmanaged MSH chassis. These settings are used when the MSH chassis containing the Switch is first powered-up. Subsequent changes made to the settings directly through the Switch's onboard management software, either via an SNMP Network Manager or using the VT100 interface, will be backed-up in non-volatile memory, and will override the manual link settings if the Switch is subsequently reset. If, however the Switch detects that the link settings have changed since the last reset, the new link setting is applied and any configuration stored in memory is deleted.

In a Managed System

In a managed MSH chassis, operation of the Switch 1005 is the same, but the Management Module may itself override the link settings. This will occur if:

- The Management Module has a stored configuration for a Switch 1005 in that slot, and the stored backplane settings are different from the set on the Switch 1005
- The Management Module derives default backplane settings that are different from the set on the Switch 1005

If the Management Module has no stored configuration data for the Switch 1005, it will apply the following default backplane settings:

- the first Switch 1005 detected in the chassis will have all backplane ports enabled.
- subsequent Switch 1005 modules will have only the Fast Ethernet backplane enabled.

To ensure that the Management Module can see and configure new Switch 1005 modules correctly when they are inserted, you must insert them when the MSH chassis and Management Module are powered on.

Setting up the Switch 1005

You can manage the Switch 1005 using any of the following methods:

- Access the VT100 interface by connecting a VT100 terminal (or workstation with terminal emulation software) to the serial port located on the front panel of a managed MSH chassis.
- Access the VT100 interface over a TCP/IP network using a workstation running VT100 terminal emulation and Telnet.
- Use an SNMP Network Manager (such as 3Com's Transcend Enterprise Manager) over a network running either the IP or IPX protocol. Each Network Manager provides its own user interface to the management facilities.

You can find further information on connecting equipment to the MSH serial port in the user documentation that accompanies the MSH Management Module.

Using the VT100 Interface

The menu-driven interface built into the Switch 1005 is known as the *VT100* or *Local Management* interface. This interface gives a forms-based structure with pre-defined security levels enabling access to be restricted to particular users. The Switch 1005 can support up to four management user sessions concurrently (for example, one serial port and three telnet connections). You can find more information about the VT100 interface in the user documentation that accompanies the Management Module, but for quick reference, Table 2-2 and Table 2-3 list the types of information found on a VT100 screen and the key sequences you can use to navigate the screens.

Table 2-2 VT100 screen components

Type of information	Shown on screen as...	Description
Choice Field	*text*	Text enclosed with markers is a list from which you can select one option only. Press [Space] to cycle through the options. Press [Down Arrow] or [Return] to move to the next field.
Entry Field	[text]	Text enclosed in square brackets on the screen is a text entry field. An entry field allows you to enter different types of data from the keyboard. This may be text, numeric data or hexadecimal data. Password fields are hidden, meaning the text you type, is not shown on the screen. In some cases an Entry Field will have a default entry. If you wish to replace the default, simply type in a new value for this field; the default entry will be erased. Press [Down Arrow] or [Return] to move to the next field.
Button	OK	Text for a button is always shown in uppercase letters. A button carries out an action. For example OK or CANCEL. To operate a button move the cursor to the button and press [Return].
List Box	monitor manager security	A List Box allows you to select one or more items from a list. There are several keys that allow you to use a List Box: ■ [Return] moves the cursor to the next field and actions your selections. ■ [Space Bar] toggles through the options in a choice field or selects and deselects an entry in the list box. List box selections will be highlighted. ■ [Down Arrow] moves item by item down the list box until it reaches the end of the list. At the end of the list it moves the cursor to the next field. ■ [Ctrl] + [U] moves the cursor one page Up the List Box. ■ [Ctrl] + [D] moves the cursor one page Down the List Box.

Table 2-3 Keyboard shortcuts

Use this key sequence...	To do this...
[Tab]	move from one field to the next, on any screen without making any changes.
[Return]	move to the next field on a form after you have made changes to the data in a field.
[Left Arrow]	move to the previous field on the screen or the next character in an editable field.
[Right Arrow]	move to the next field on the screen or the previous character in an editable field.
[Ctrl] + [R]	refresh the screen.
[Ctrl] + [B]	move the cursor to the next Button.
[Ctrl] + [P]	abort the current screen and return to the previous screen.
[Ctrl] + [N]	action the inputs for the current screen and move to the next screen.
[Ctrl] + [K]	display a list of the available key strokes.
[Delete] or [Backspace]	move the cursor one space to the left and delete a character. To delete several characters, press the key several times.

If you are using Telnet or a terminal emulation program you may find that some of the Control keys do not operate or that they activate other functions. Check carefully in the manual accompanying your Telnet or terminal emulation software before using the Control keys.

Using Telnet

Once you have specified the module's IP parameters, you can use any Telnet application that emulates a VT100 terminal to communicate with it over the network. To open a Telnet session, specify the IP address of the Switch 1005. For example:

```
telnet 191.120.131.6
```

For further information on using Telnet, refer to the documentation supplied with the application.

Up to three active Telnet sessions can access the Switch 1005 concurrently. If a connection to a Telnet session is lost inadvertently, the connection is closed by the Switch 1005 after 2 to 3 minutes of inactivity.

Using an SNMP Network Manager

Once you have set up the IP parameters of the Switch 1005, you can use any SNMP Network Manager for in-band management, provided the Management Information Base (MIB) is correctly installed at your network management station.

3Com provides the Transcend range of SNMP Network Managers, the use of which is not described in this User Guide; refer to the User Guides that accompany the software. To manage the Switch 1005 with a Network Manager from another vendor, you will need to ensure you have the correct MIB. Contact your local support representative for advice.

Accessing the Switch 1005 VT100 Interface

The following sections explain how to access the VT100 management screens for the Switch 1005. You may find it useful to refer to Figure 2-2 when locating the screens you require.

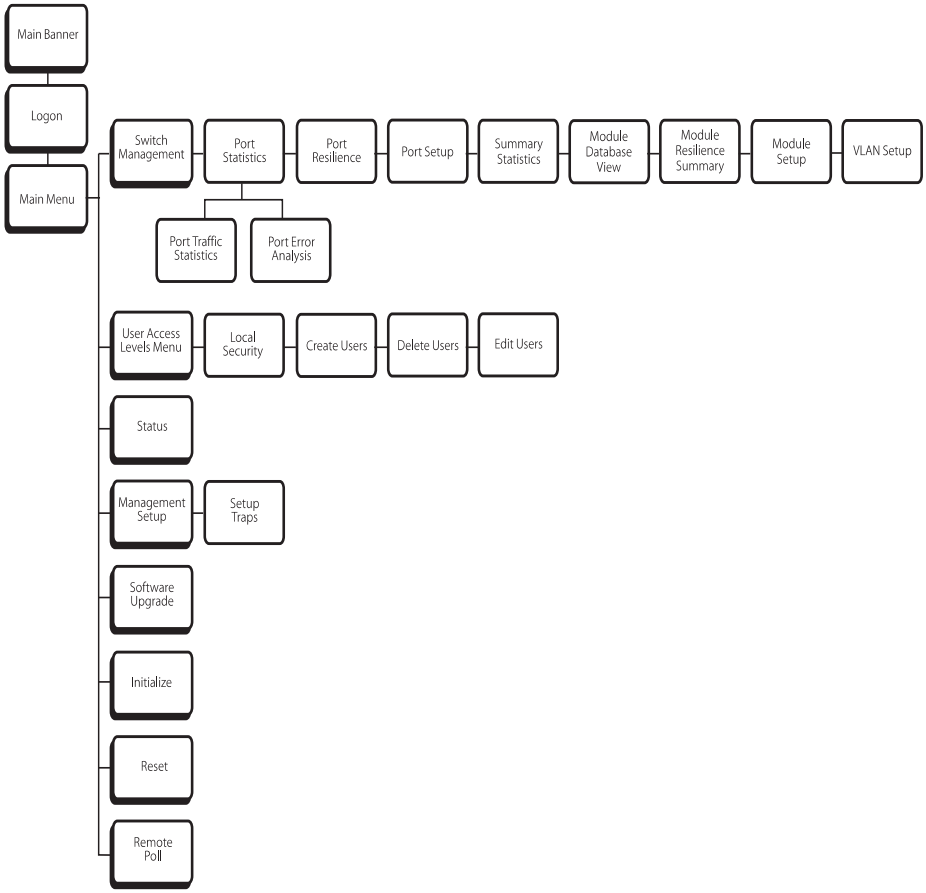


Figure 2-2 VT100 screen map

Logging On

1. Logon to the LinkBuilder MSH. This is described fully in the *LinkBuilder MSH Management Module (3C18500) User Guide*, part number DUA1850-0AAA0x.

2. When you have successfully logged on to the MSH, you will see the 3Com LinkBuilder Main Menu. From the list of options, select SERVICE SELECTION.

3. From the list of services available for this MSH, select Switch 1005; the LinkBuilder MSH Address Table appears. Choose the Switch 1005 you wish to setup and select the MANAGE button. The Switch Main Banner screen appears.

4. From the Switch 1005 Main Banner screen, press [Return] to display the Logon screen shown in Figure 2-3.

5. Enter your user name and password. Note that they are both case-sensitive.

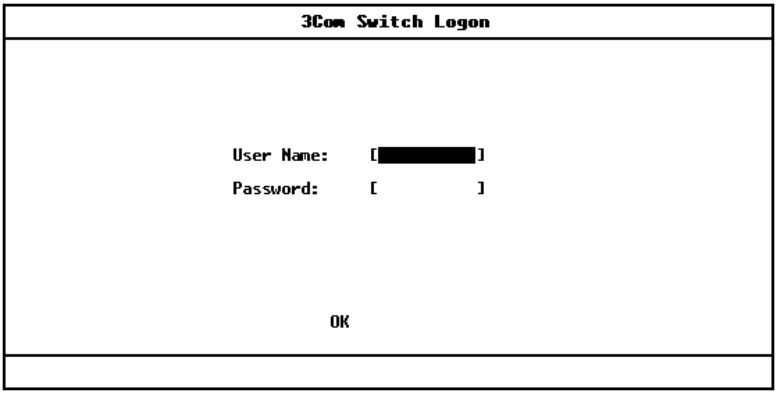


Figure 2-3 Switch 1005 Logon screen

- If you are logging on for the first time (after installation or initialization), use a default user name and password to match your access requirements. We recommend you that you use the default user *security* so that you can access all functions. The defaults are shown in Table 2-4 below.
- If you have been assigned a user name, access level and password, enter those details.

Table 2-4 Default Users

User Name	Default Password	Access Level
monitor	monitor	monitor - this user can view but not change, a subset of the manageable parameters
manager	manager	manager - this user can access and change the operational parameters but not special/security features
security	security	security - this user can access and change all manageable parameters

After Logging On

When you have successfully logged on to the Switch 1005, the Main Menu appears as shown in Figure 2-4.

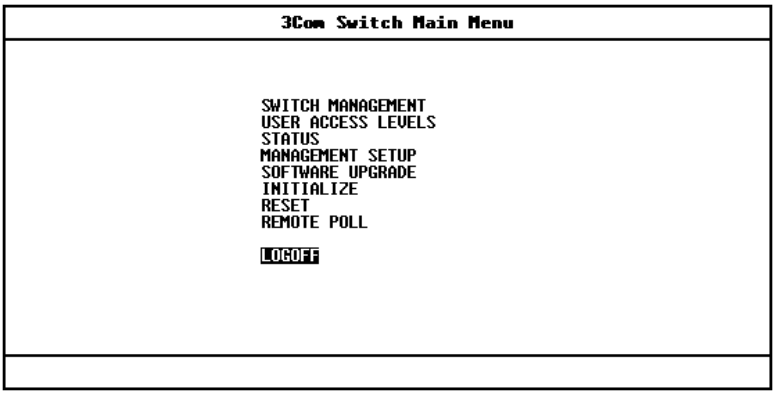


Figure 2-4 Switch 1005 Main Menu

From here, you can select the options needed to manage the module.

Access to options depends on the access level you have been assigned. Access rights to the VT100 screens for the Switch 1005 are listed in Appendix A.

If you are a user with *security* access level, and are using the management facility for the first time, we suggest that you:

- Assign a new password for the *security* access level as described in "Editing User Details" on page 2-23.
- Assign new passwords for the other default users as described in "Editing User Details" on page 2-23.
- Set up user names and passwords for any other users, and assign each user an appropriate security level as described in "Creating a New User" on page 2-21.

You should select the MANAGEMENT SETUP option to assign IP parameters. This is described in the following section.

Switch 1005 Management Setup

The Switch Management Setup screen allows you to configure IP and IPX parameters for the Switch 1005. This screen also allows you to display a screen for setting up traps.

If you change the IP parameters using this screen, the changes will not take effect until you reset the Switch 1005. Refer to "Resetting the Switch 1005" in Chapter 3.

To access the Setup screen, from the Switch Main Menu screen, select the MANAGEMENT SETUP option. The Setup screen appears as shown in Figure 2-5.

```
                    3Com Switch Management Setup

MAC Address:                  08004E0AB30D

Power On Self Test Type:    ◇Normal  ◇

Device IP Address: [161.71.51.151  ]
Device SubNet Mask:[255.255.255.0  ]
Default Router:    [161.71.51.20   ]
BOOTP Select:      ◇Enabled ◇

IPX Network  Node           Status    Data Link Protocol
[00356501] : 08004e0ab30d  ◇Enabled ◇ Ethernet_802.3
[00356502] : 08004e0ab30d  ◇Enabled ◇ Ethernet_802.2
[00356503] : 08004e0ab30d  ◇Enabled ◇ Ethernet_II
[00356504] : 08004e0ab30d  ◇Enabled ◇ Ethernet_SNAP

                OK    SETUP TRAPS                CANCEL
```

Figure 2-5 Switch Management Setup screen

The screen shows the following:

MAC Address The Switch 1005 MAC address required for management.

Power On Self Test (POST) Type *Normal/Extended* Use this field to determine the type of self-test that the Switch 1005 carries out when it is powered up. If this field is set to *Normal*, a basic confidence check lasting approximately 10 seconds is carried out. If this field is set to *Extended*, a full set of tests are carried out which may take up to 90 seconds to complete.

Device IP Address If using IP, a unique IP address must be specified in this field. If you do not know your IP address, consult your network administrator. You can change the IP address using this field; for the change to take effect, you must reset the Switch 1005.

Device SubNet Mask If using IP, type in a suitable network mask. For a class B IP address, 255.255.0.0 is suitable. For more information, see your network administrator. You can change the Device SubNet Mask using this field; for the change to take effect, you must reset the Switch.

Default Router If a default router exists on your network, type in the IP address here. You can change the Device Router IP address using this field; for the change to take effect, you must reset the Switch 1005.

BOOTP Select *Enabled/Disabled* If BOOTP is enabled and you have a BOOTP server on your network, an IP address will be automatically mapped to the Switch when it is first powered up. In addition to mapping an IP address, BOOTP can assign the subnet mask and default router. Using a BOOTP server avoids having to configure devices individually.

There are four entries under the following four fields; one for each data link layer protocol that can be used by IPX.

IPX Network This field shows the address of the network for this protocol. This address is learned automatically from the local IPX router or Netware file server, and you do not need to change it.

Node This read-only field shows the node address of the Switch 1005 which is learned automatically.

Status *Enabled/Disabled* If this field is set to *Enabled*, the Switch 1005 supports SNMP over IPX. For security, set this field to *Disabled* if you do not require SNMP over IPX.

Data Link Protocol This field shows the name of the IPX data link layer protocol.

SETUP TRAPS Select this button to display the setup screen for trap parameters. Trap Setup is described in "Setting Up Traps" in Chapter 3.

Logging Off

If you have finished using the facility, select the Logoff option from the bottom of the main menu. If you accessed the facility using a Telnet session or modem connection, the connection will be closed automatically.

Auto Logout

There is a built-in security timeout on the VT100 interface. If you do not press any keys for three minutes, the management facility will warn you that the inactivity timer is about to expire. If you do not press a key within 10 seconds, the timer will expire and the screen will be locked; any displayed statistics will continue to be updated. When you next press a key, the display changes to the Auto Logout screen shown in Figure 2-6.

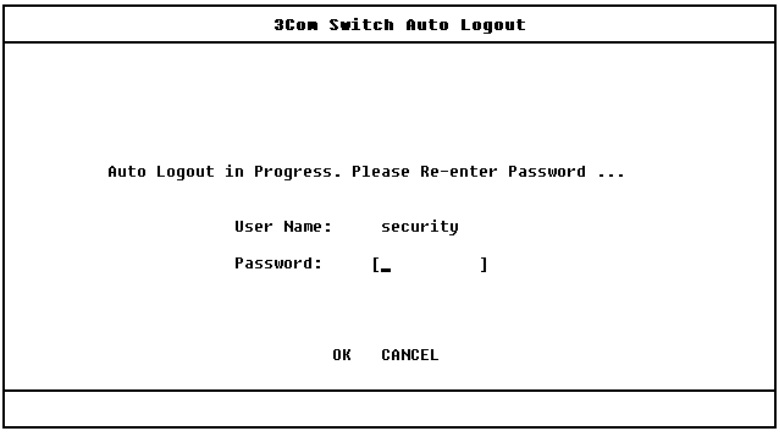


Figure 2-6 Auto Logout screen

The Auto Logout screen requests you to enter your password again. If the password is correctly entered, the screen that was active when the timer expired is displayed. If you make a mistake entering your password, you will be returned to the Logon screen.

If you connected to the Switch 1005 via the MSH Management Module screens, the LinkBuilder MSH Address Table screen is displayed once you have entered the correct password.

Setting Up Users

From the Main Menu, select USER ACCESS LEVELS. The User Access Levels screen appears as shown in Figure 2-7.

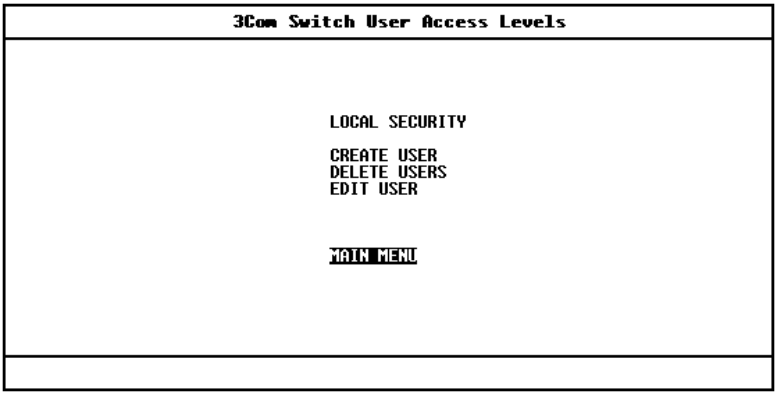


Figure 2-7 User Access Levels screen

From this screen you can access:

- **LOCAL SECURITY screen** — Lets you set up access levels for users on the Switch 1005.
- **CREATE USER screen** — In addition to the default users set up on the Switch 1005, you can add up to ten new users.
- **DELETE USERS screen** — Lets you delete users from the Switch 1005. The default users cannot be deleted.
- **EDIT USER screen** — Lets you change your own password and community string. You cannot change details for other users.

Creating a New User

These steps assume the User Access Levels screen is displayed.

1 Select the CREATE USER option. The Create User screen appears as shown in Figure 2-8.

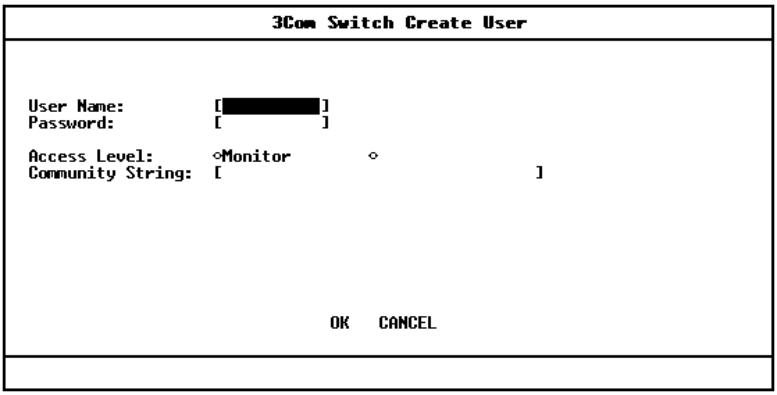


Figure 2-8 Create User screen

2 Fill in the fields and assign an access level for the new user.

3 When the form is completed, select OK

The Create User screen shows the following fields:

User Name Type in the name of this new user. The name can consist of up to 10 characters and is case-sensitive.

Password Type in the password for this new user. The password can consist of up to 10 characters and is case-sensitive. For security reasons, the password is not displayed on screen.

Access Level Assign an access level for this new user, as follows:

- *monitor* — access to view, but not change a subset of the manageable parameters of the Switch 1005
- *secure monitor* — as *monitor*

- *manager* — access to all the manageable parameters of the Switch 1005, except security features
- *specialist* — as *manager*
- *security* — access to all manageable parameters of the Switch 1005

Community String By default a community string identical to the user name is generated. You can change this to any text string of 32 characters or less. The community string is only needed for SNMP access. If you are using a remote SNMP network manager, the community string specified in the Network Manager's database must be the same as that for the device.

Deleting a User

These steps assume the User Access Levels screen is displayed.

1 Select the DELETE USER option. The Delete Users screen appears as shown in Figure 2-9.

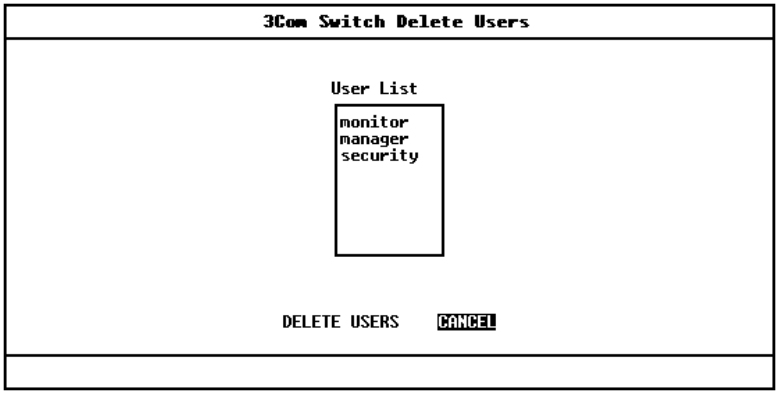


Figure 2-9 Delete Users screen

2 Use the spacebar to highlight the user that you want to delete. Note that you cannot delete default users or the current user (that is, yourself).

3 Select DELETE USERS.

Editing User Details

These steps assume the User Access Levels screen is displayed.

1 Select the EDIT USER option. The Edit User screen appears as shown in Figure 2-10.

Figure 2-10 Edit User screen

2 Fill in the fields as required.

3 When you have completed the changes, select OK.

The Edit User screen shows the following fields:

User Name This read-only field shows the name of the user. This field cannot be changed; if you need to change the user name, you must delete this user and create a new one.

Old Password Type in the old password for this user.

New Password Type in a new password for this user.

Confirm Password Retype the new password into this field.

Community String Type a new community string into this field.

If you forget your password while logged out of the Switch 1005 VT100 interface, contact your local technical support representative who will advise on your next course of action.

Assigning Local Security

The local security screen shows a matrix of options for access method (Serial Port, Remote Telnet, Community-SNMP) and access level.

These steps assume the User Access Levels screen is displayed.

1 Select the LOCAL SECURITY option. The Local Security screen appears as shown in Figure 2-11.

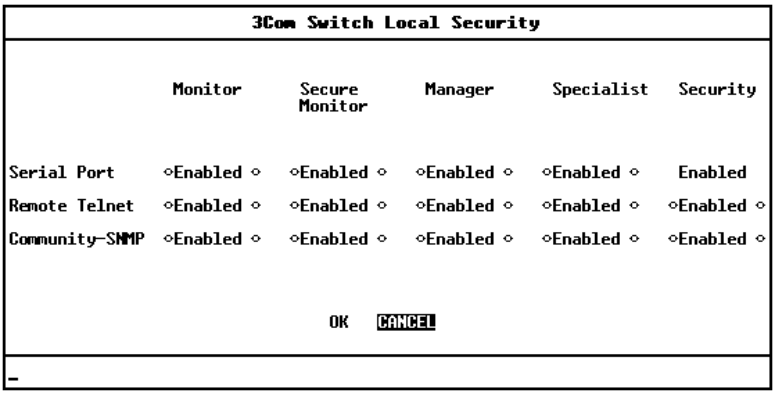


Figure 2-11 Switch Local Security screen

2 Fill in the fields as required.

3 When you have filled in the form, select OK.

Options for the access methods are:

Serial Port *Enabled/Disabled* To prevent access to the management facilities via the serial port, disable access to the facility for each access level. Serial Port access for *Security* is enabled and cannot be changed. This prevents accidental disabling of all access levels from management.

Remote Telnet *Enabled/Disabled* Telnet is an insecure protocol. You may want to disable all access to the management facilities via Telnet if there is important or sensitive data on your network.

Community SNMP *Enabled/Disabled* The Switch 1005 can be managed via SNMP using a remote network manager. Community SNMP does have some simple security features, but it is an insecure protocol. You may want to disable all access to the management facilities if there is important or sensitive data on your network.

3 SWITCH CONFIGURATION

Choosing a Switch Management Level

The Switch Management screen lets you:

- Choose between managing a port, the Switch module or a VLAN.
- Display screens showing statistical information.
- Display the Switch Database configuration screen.
- Display the Switch Unit Resilience Summary screen.
- Display Setup screens for the Switch 1005.

From the Main Menu, select SWITCH MANAGEMENT. The Switch Management screen appears as shown in Figure 3-1.

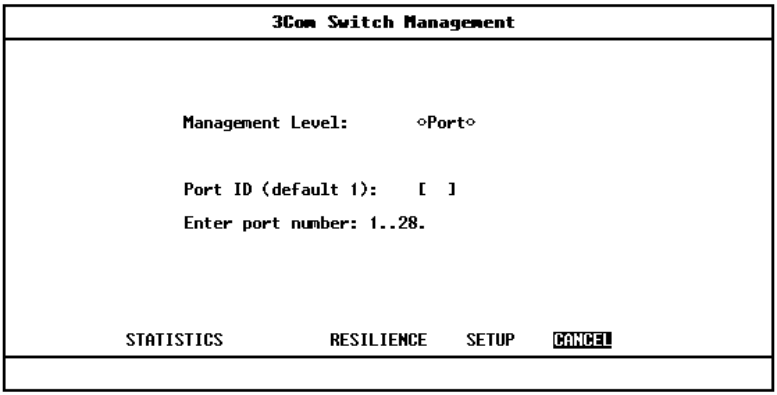


Figure 3-1 Switch Management screen — port level

Management Level *Module/Port/VLAN* If you choose *Module*, the screen that appears is similar to the example shown in Figure 3-2 and all options at the foot of the screen relate to the Switch 1005. If you choose *Port*, the screen that appears is similar to that shown in Figure 3-1 and all options relate to an individual port. If you choose *VLAN*, the screen that appears is similar to that shown in Figure 3-3 and all options relate to VLANs.

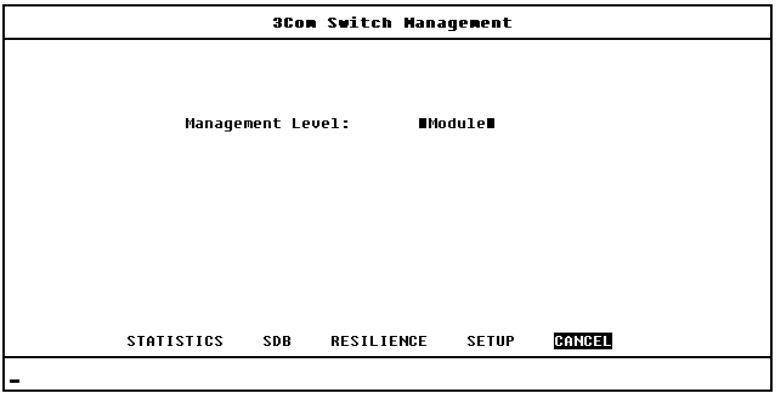


Figure 3-2 Switch Management screen — module level

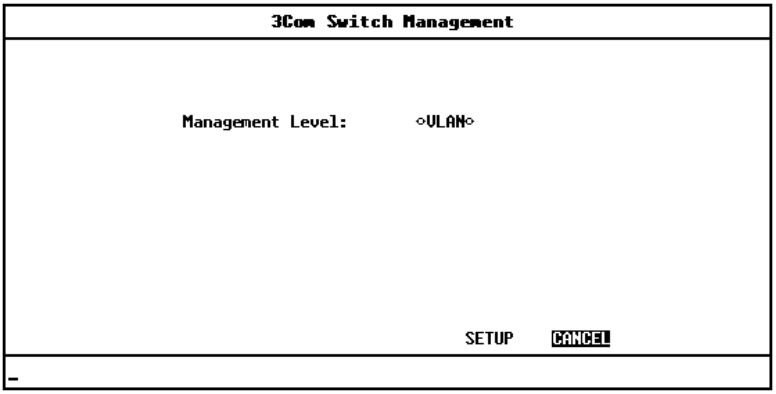


Figure 3-3 Switch Management screen — VLAN level

Port ID *1 ... 28* When managing a Switch 1005 *port*, type the port number into this field before selecting the next screen:

- Ports 1 to 4 represent ports on any Transceiver Module you may have installed
- Ports 5 to 12 are the eight fixed 10BASE-T port
- Ports 12 to 24 are additional ports you may have if you have installed an Expansion Module
- Ports 25 to 27 are internal Ethernet backplane ports (10Mbps)
- Port 28 is the internal Fast Ethernet backplane (100Mbps)

STATISTICS Use this button to display statistics screens for the level of management you have chosen (module, port or VLAN). See Chapter 5.

SDB Use this button to display the Switch Database Configuration screen. See "Configuring the Switch Database" on page 3-14.

RESILIENCE Use this button to display the resilience screen for the module or specified port. See "Resilient Links" on page 3-17.

SETUP Use this button to display configuration screens for the level of management you have chosen (module, port or VLAN). For information about the Switch Module Setup and Port Setup screens, see "Switch 1005 Setup" and "Port Setup" later in this chapter. Setting up VLANs is described in Chapter 4.

Switch 1005 Setup

With the Switch Management screen displayed, choose to setup the *module*, then select the SETUP button.

The Switch Module Setup screen is displayed as shown in Figure 3-4.

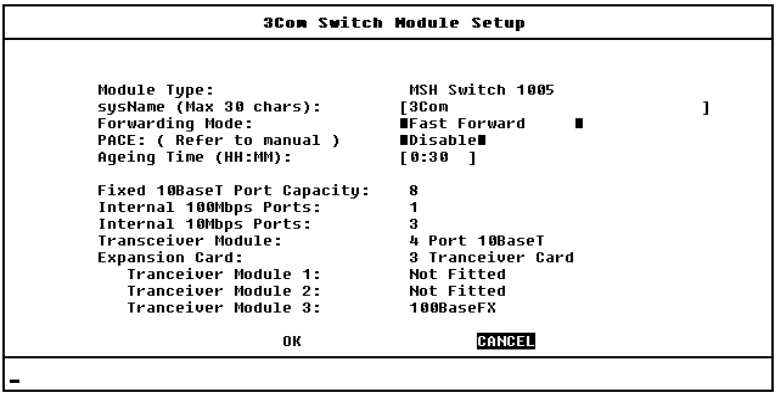


Figure 3-4 Module Setup screen

The screen shows the following:

Module Type A read-only field showing the type of device.

sysName This field takes its name from the MIB II System Group object. You can edit the first 30 characters of this field to make the name more meaningful. This name is displayed on the Main Banner when you first access the VT100 screens, and is also accessible to an SNMP Network Manager.

Forwarding Mode *Fast Forward/Fragment Free/Store and Forward/Intelligent* This field allows you to set the forwarding mode:

- *Fast Forward* — In this mode, frames are forwarded as soon as the destination address is received and verified. The forwarding delay or latency for all frames in this mode is 40µs, but with no checking time any collision fragments or error frames are propagated onto the network.

- *Fragment Free* — In this mode, a minimum of 64 bytes of the received frame is buffered prior to the frame being forwarded. This ensures that collision fragments are not propagated through the network, however, CRC errors are forwarded. The forwarding delay or latency for all frames in this mode is 64µs.
- *Store and Forward* — In this mode, received packets are buffered in their entirety prior to forwarding. This ensures that only good frames are passed to their destination. The forwarding delay for this mode varies between 64µs and 1.2ms, depending on frame length. In this mode the latency, measured as the time between receiving the last bit of the frame and transmitting the first bit, is 8µs.
- *Intelligent* — In this mode, the Switch 1005 monitors the amount of error traffic on the network and changes the forwarding mode accordingly. If the Switch 1005 detects less than 18 error packets per second, it will operate in Fast Forward mode. If the Switch 1005 detects more than 18 packets per second it will operate in Store and Forward mode until the number of error packers per second returns to 0.

PACE *Enable/Disable* This field allows you to enable or disable PACE (Priority Access Control Enabled) for all ports on the Switch 1005. Enabling PACE on a port increases network performance, especially if you are running multimedia applications. The rules for enabling PACE are:

- PACE should only be enabled on ports that connect to a single end-station, switch, bridge or router
- You should not enable PACE on a port connected to a repeater
- If you have PACE-equipped devices at both ends of a link, PACE should only be enabled on *one* of the devices

Ageing Time This field allows you to specify the ageing time (hours:minutes) for all non-permanent entries in the Switch Database of the module You can set an ageing time in the range 0 minutes to 277 hours with a default of 30 minutes. If you enter 00:00, the database entries are non-ageing; non-ageing entries do not age but will be deleted from the database if the Switch 1005 is reset or a power-off/on cycle occurs.

Fixed 10BaseT Port Capacity This read-only field shows how many non-removable Ethernet ports (10Mbps) are on this module.

Internal 100Mbps Ports This read-only field shows how many internal connections to the Fast Ethernet (100Mbps) backplane are available for this module.

Internal 10Mbps Ports This read-only field shows how many internal connections to the Ethernet backplane (10Mbps) are available for this module.

Transceiver Module This read-only field shows the type of Transceiver Module installed into the module, or states *Not Fitted*.

Expansion Card This read-only field shows the type of Expansion Module fitted onto this module, or states *Not Fitted*.

Transceiver Module 1, **Transceiver Module 2**, **Transceiver Module 3** These three read-only fields show the type of Transceiver Modules installed into your Expansion Module (if fitted), or state *Not Fitted*.

Port Setup

With the Switch Management screen displayed, choose to setup the *port*, then select the SETUP button.

The Switch Port Setup screen is displayed as shown in Figure 3-5.

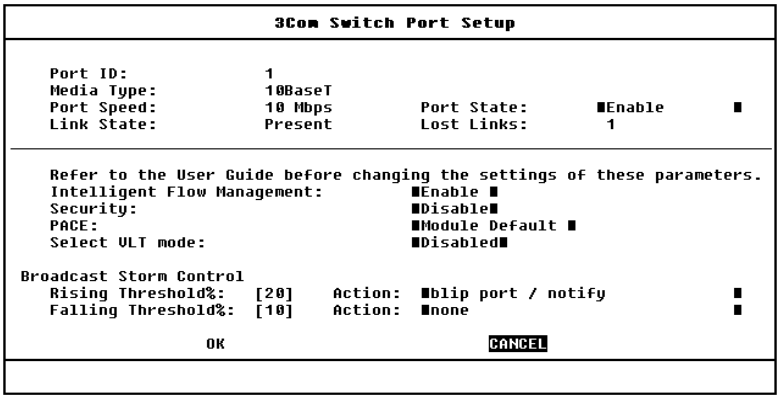


Figure 3-5 Port Setup screen

The screen shows the following:

Port ID This read-only field shows the ID of the port you have chosen to setup.

Media Type This read-only field shows the media type of the link connected to the port.

Port Speed This read-only field shows the speed of the link.

Link State *Present/Not Available* For twisted pair and fiber ports only, this read-only field shows the state of the link:

- *Present* — The port is operating normally.
- *Not Available* — The link has been lost.

Port State *Enable/Disable* This option allows you to enable/disable the port. To prevent unauthorized access, we recommend that you disable any unused ports.

Lost Links The number of times the link has been lost since the Switch 1005 was last reset. If this field displays a number other than 0, you should check your cables and replace any that may be damaged.

If the port is directly connected to an end-station, this counter increments each time the end-station goes through a power off/on cycle and is not a result of faulty cabling.

Intelligent Flow Management (IFM) *Enable/Disable* This option allows you to enable or disable IFM. IFM minimizes packet loss which can occur with conventional switches.

Intelligent Flow Management (IFM) should be disabled if the port is connected to a repeated segment where the traffic is local to that segment.

Security *Enable/Disable* When Security is enabled, the port enters a single address learning mode. The Switch 1005 removes all addresses currently stored against the port in the Switch Database. The Switch 1005 then learns the source address from the first packet it receives on the port since security was enabled. The port then enters a secure mode. Once security is enabled, no other station with a different address is permitted to access the network through the secure port. If a station with a different address attempts to transmit packets through onto the network through the port, the port is automatically disabled and a trap is generated. The port remains disabled until it is enabled using this screen or an SNMP Network Manager.

Security is not available on backbone ports. If the port has been defined as a backbone port, the Security field will not be displayed.

PACE *Enable/Disable/Unit Default* This field allows you to enable or disable PACE (Priority Access Control Enabled) on the port:

- *Enable* — Enabling PACE increases network performance particularly if you are using multimedia applications. You should only enable PACE on a port if it is connected to a single end-station, switch, bridge or router. Setting this field overrides the PACE configuration specified for the port using the Module Setup screen, see "Switch 1005 Setup" starting on page 3-4.
- *Disable* — You should disable PACE if the port connects to a repeater.
- *Unit Default* — The PACE mode for the port is determined by the unit setting configured on the Module Setup screen, see "Switch 1005 Setup" on page 3-4.

Select VLT Mode *Enable/Disable* This field allows you to specify whether the port forms part of a Virtual LAN Trunk (VLT). A Virtual LAN Trunk is a connection which carries traffic for multiple VLANs between Switch 1005 modules. You can find more information about VLANs in Chapter 5.

Duplex Mode *Half Duplex/Full Duplex* This field allows you to enable full duplex on Fast Ethernet ports:

- *Full Duplex* — Full duplex allows packets to be transmitted and received simultaneously and, in effect, doubles the bandwidth available on a Fast Ethernet link. For 100BASE-FX links, full duplex also allows cable runs of up to 2km. You should only enable full duplex on a point to point link between the Switch and another device with full duplex support.
- *Half Duplex* — You should use half duplex if the port connects to a shared Ethernet LAN segment, or if the device at the other end of a point to point link does not support full duplex.

Intelligent Flow Management (IFM) will not work on a port which uses full duplex, therefore the Intelligent Flow Management field will be disabled if full duplex is enabled.

Broadcast Storm Control The Switch 1005 automatically creates an alarm on each of its ports to monitor the level of broadcast traffic on each port. The Broadcast Storm Control fields allow you to specify thresholds for the level of broadcast traffic on a port. In addition, you can specify an action to take place if the threshold is exceeded.

Rising Threshold% The value entered here is the percentage bandwidth of traffic using a broadcast address that will be reached before you are notified. The default is 20%.

Falling Threshold% The value entered here is the percentage bandwidth of traffic using a broadcast address at which the alarm trigger will be reset. This prevents the rising threshold events being triggered continuously. The default is 10%.

Rising Action *none / event / disable port / disable port/notify / blip / blip port/notify* Use this field to specify the action for the alarm to take when it reaches the rising threshold:

- *none* — no action takes place
- *event* — an SNMP trap is generated
- *disable port* — the port is disabled
- *disable port/notify* — the port is disabled and an SNMP trap is generated
- *blip* — the port is disabled, then enabled after 5 seconds
- *blip port/notify* — the port is disabled, then enabled after 5 seconds and an SNMP trap is generated

Falling Action *none/event/enable/event + enable* Use this field to specify the action for the alarm to take when it reaches the falling threshold:

- *none* — no action takes place
- *event* — an SNMP trap is generated
- *enable* — the port is enabled
- *event + enable* — the port is enabled and an SNMP trap is generated

You should be aware of the following points when using Broadcast Storm Control:

- *The Switch takes 5-7 seconds to recognize that a broadcast storm is occurring.*
- *Broadcast Storm Control calculates the average broadcast bandwidth over the previous 20 second interval. The average is based on 4 samples which are taken at 5 second intervals.*
- *When the average value exceeds the rising threshold value, the rising action is triggered. The action will not be triggered again until the average broadcast bandwidth falls below the falling threshold level.*

Specifying the Backbone Port

Specifying the backbone port for your Switch 1005 is carried out through the VLAN Setup screen. Refer to "Specifying a Backbone Port" in Chapter 4

The Switch Database (SDB)

The Switch 1005 maintains a database of all addresses received on all of its local ports. It uses the information in this database to decide whether a frame should be forwarded or filtered. The database holds up to a maximum of 500 entries, each entry consists of the MAC address of the device and an identifier for the port on which it was received.

If you have set up Traps for the Switch 1005, notification that the database is becoming full is provided by two traps:

- *Database is 90% full*
- *Database is 100% full*

These traps indicate that the maximum number of devices which can be attached to the Switch 1005 has been reached. You cannot connect any more devices to the Switch 1005, however, additional devices can be connected to the rest of the network infrastructure.

Entries are added into the SDB in two ways:

- The module can learn entries, that is, the unit updates the SDB with the source MAC address and the port identifier on which the source MAC address is seen.
- The system administrator can enter and update entries using a MIB browser, an SNMP Network Manager, or the Switch Database screen described over the following pages.

There are two types of entries in the SDB:

- **Ageing entries** — Initially, all entries in the database are of type Ageing. Entries in the database are removed (aged) if, after a period of time (ageing time), the device has not transmitted. This prevents the database from becoming full with obsolete entries by ensuring that when a device is removed from the network, its entry is deleted from the database. Ageing entries are deleted from the database if the Switch 1005 is reset or a power off/on cycle occurs. For more information about setting an ageing time, see "Switch 1005 Setup" on page 3-4.

- **Non-ageing entries** — If the ageing time is set to 00:00, all ageing entries in the database are defined as non-ageing entries. This means that they do not age, but they are still deleted if the Switch 1005 is reset. For more information about setting an ageing time, see see "Switch 1005 Setup" on page 3-4.
- **Permanent entries** — Permanent entries are retained in the database if the Switch 1005 is reset or a power off/on cycle occurs. It is up to the system administrator to make entries permanent. You can do this with single addresses or all addresses in the database using an SNMP Network Manager. All entries entered via the switch database are stored as permanent.

Configuring the Switch Database

The Switch Module Database View screen, shown in Figure 3-6, allows you to display and configure the contents of the Switch 1005 database.

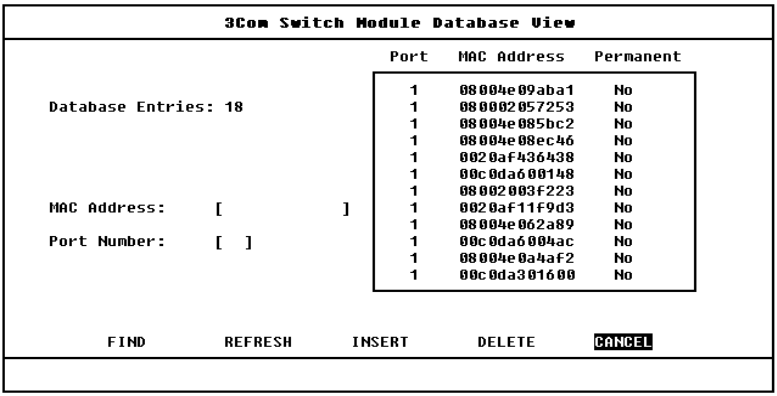


Figure 3-6 Switch Module Database View screen

To access the screen, make sure the Switch Management screen is displayed, see "Choosing a Switch Management Level" on page 3-1. From the foot of the screen select the SDB button.

The screen shows the following:

Database Entries This read-only field shows the number of entries currently in the SDB. The database holds a maximum of 500 addresses.

MAC Address If an entry in the listbox is highlighted and you press [Return], this field shows the device MAC address for this entry.

Port Number If an entry is highlighted in the listbox, this field shows the port identifier for this entry.

A listbox containing the following three fields:

Port The port ID for this entry.

MAC Address The MAC address for the port currently stored in the database.

Permanent Shows Yes if this entry is *permanent*, or No if this entry is *ageing*. See the previous section "The Switch Database (SDB)" for a description of permanent and ageing entries.

FIND This button lets you locate an entry in the database.

REFRESH This button refreshes the database so that it displays the latest information.

INSERT This button lets you insert an entry into the database.

DELETE This button allows you to delete entries from the database.

Searching the Switch Database

You can search the switch database in two ways; by MAC address or port number.

By MAC Address

To locate the port number against which a particular MAC address is entered in the SDB:

1. In the *MAC Address* field, type in the MAC address you are trying to locate.
2. Select FIND. The port ID is displayed in the *Port Number* field and the entry in the listbox is highlighted with a star (*).

By Port

To locate the MAC addresses entered against a particular port in the SDB:

1. Clear the *MAC Address* field by moving into the field and pressing the [Space] bar.

2 In the *Port Number* field, enter the port ID for which you want MAC addresses displayed.

3 Select FIND. The listbox will show entries in the database for that port only.

Adding an Entry into the SDB

1 In the *MAC Address* field, type in the MAC address of the device.

2 In the *Port Number* field, type in the port identifier for this device.

3 Select INSERT. Entries inserted this way are permanent entries.

Deleting an Entry from the SDB

1 In the listbox, highlight the entry you want to delete and press [Return], or type the MAC address into the MAC Address field.

2 Select DELETE.

Resilient Links

Switch 1005 ports can be configured to provide resilient links. A resilient link consists of a main link and a standby link. Under normal network operating conditions, the main link carries your data. The fiber Receive Idle signal or the Test Pulse on twisted pair links is continually monitored by the management software. If a signal loss is detected, management software immediately enables the standby port so that it carries the data and network disruption is minimized. In addition, the main port is disabled.

When setting up resilient links, you should note the following:

- Up to 12 resilient link pairs can be configured on the Switch 1005.
- The main and standby ports must be set up on the same Switch 1005 or module pair (main module with fitted expansion module).
- Resilient links can be set up on any of the external ports.
- Resilient links can only be set up on fiber or twisted pair links. The main and standby links in the same pair however, can use any combination of these media or speed (10Mbps/100Mbps).
- A backbone port can be configured as a main port in a resilient link pair. If a resilient backbone port fails, the standby port is immediately configured as a backbone port before it is enabled. A backbone port cannot be configured as a standby port.
- Both ports must have an identical security setup.
- Both ports must belong to the same VLAN.
- You cannot disable any port that is part of a resilient link pair.
- The resilient link must only be defined at one end of the link.
- A resilient link can only be set up if neither of the ports already form part of another resilient link pair.
- If an active standby link fails and there is a link on the main port, the main port will be enabled and the standby port will be disabled.

Viewing Resilient Setup

With the Switch Management screen displayed, choose to set up the *module* and select the RESILIENCE button.

The Switch Module Resilience Summary screen is displayed as shown in Figure 3-7. This screen shows the current resilient link configuration for the module.

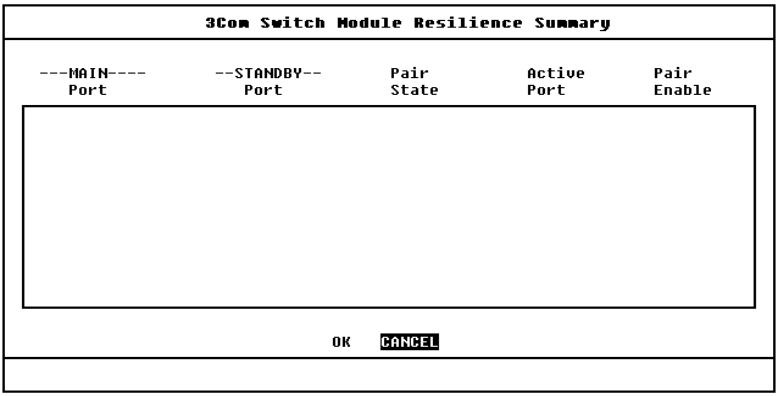


Figure 3-7 Module Resilience Summary screen

The following read-only information is displayed:

MAIN Port The ID of the port configured as the main port for this resilient link pair.

STANDBY Port The ID of the port configured as the standby port for this resilient link pair.

Pair State *Active/Both Failed/Unknown/Not Available* The current operating state of this resilient link pair:

- *Active* — The resilient link pair is enabled and operating normally with both main and standby port capable of carrying traffic.
- *Both Failed* — Although the resilient link is correctly configured, both links have failed. This could be due to loose connections or cable damage.

- *Unknown* — The network configuration has changed and the resilient link pair no longer conforms to the rules.
- *Not Available* — This resilient link pair is disabled.

Active Port *Main/Standby/Both Failed* Shows which port in the resilient link pair is currently carrying traffic:

- *Main* — The pair is operating in its normal state with the main port carrying traffic.
- *Standby* — The main port has failed and the standby port is carrying the traffic. You should rectify the fault and switch operation back to the main link as soon as possible. Swapping the main and standby ports is not carried out automatically. Use the Port Resilience screen described in the next section to swap the main and standby ports.
- *Both Failed* — Both ports of the resilient link pair have failed. This could be due to loose connections or cable damage.

Pair Enable *Enabled/Disabled* States whether this resilient link pair is currently enabled or disabled. You enable or disable a resilient link pair using the Switch Port Resilience screen described in the following section.

Configuring Resilient Links

With the Switch Management screen displayed, choose the port that will be set up as the main port in the resilient link pair, then select the RESILIENCE button.

The Port Resilience screen is displayed as shown in Figure 3-8. This screen allows you to setup, edit and delete resilient link pairs.

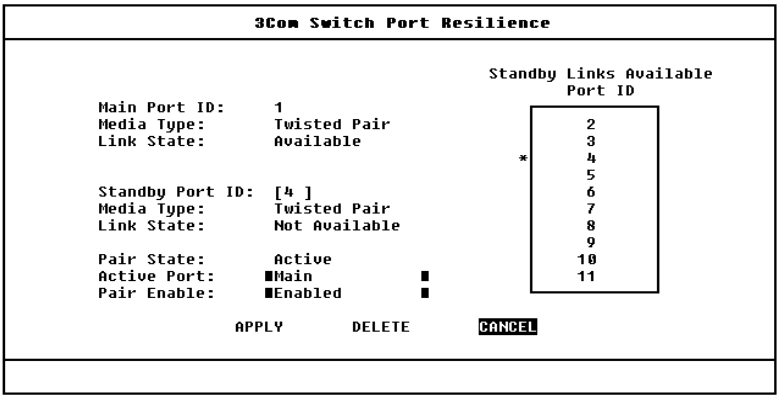


Figure 3-8 Port Resilience screen

The screen shows the following:

Main Port ID The identifier for the main port.

Media Type *Twisted Pair/Fiber* This read-only field shows the media type connected to the main port.

Link State *Available/Not Available/Not Present* This read-only field shows the connection state of the main port in the link:

- *Available* — The port is operating normally
- *Not Available* — The resilient link pair is disabled.
- *Not Present* — The port is not present in the current hardware.

Standby Port ID This field shows you the current standby port ID and allows you to enter a new ID.

Media Type *Twisted Pair/Fiber* This read-only field shows the standby port media type.

Link State *Available/Not Available/Not Present* This read-only field hows the connection state of the standby port in the link:

- *Available* — The port is operating normally.
- *Not Available* — The resilient link pair is disabled.
- *Not Present* — The port is not present in the current hardware.

Standby Links Available This listbox shows the ports that are available to set up as standby.

Pair State *Active/Both Failed/Unknown/Not Available* This read-only field shows the current operating state of the resilient link pair:

- *Active* — The resilient link pair is enabled and operating normally with both main and standby port capable of carrying traffic.
- *Both Failed* — Although the resilient link is correctly configured, both links have failed. This could be due to loose connections or cable damage.
- *Unknown* — The network configuration has changed and the resilient link pair no longer conforms to the rules.
- *Not Available* — The resilient link pair is disabled.

Active Port *Main/Standby* If your main link fails and the standby link takes over the traffic, the link will not automatically switch back when the main link is reinstated. Use this field to manually switch traffic back to the main link.

Pair Enable *Enabled/Disabled* Use this field to enable or disable the resilient link pair. If you disable the resilient link pair, you must remove cabling from the ports to avoid creating loops in your network configuration.

Creating a Resilient Link

1. Ensure that the port nominated as the standby port is not physically connected to the unit.
2. Ensure both ports have an identical port security mode configuration and that they are members of the same VLAN.
3. At the Switch Management screen, select the port to be configured as the main port in the link. Select the RESILIENCE button at the foot of the screen.
4. Select the standby port from the *Standby Links Available* listbox or enter the port ID in the *Standby Port ID* field.
5. Enable the pair in the *Pair Enabled* field. Select APPLY.
6. Connect the cabling for the standby port.

Deleting a Resilient Link

To delete the resilient link pair set up on the port, select the DELETE button at the foot of the screen. The Port Resilience screen closes and the Switch Management screen is displayed.

Setting Up Traps

Traps are messages sent across the network to an SNMP Network Manager. They alert the network administrator to faults or changes at the Switch 1005.

Your Network Manager may automatically set up traps in the Switch 1005 Trap Table. Check the documentation accompanying the network management software.

To access the Trap Setup screen, from the Switch 1005 Management Setup screen (described in "Setting up the Switch 1005" in Chapter 2), select the SETUP TRAPS button. The Trap Setup screen is shown in Figure 3-9.

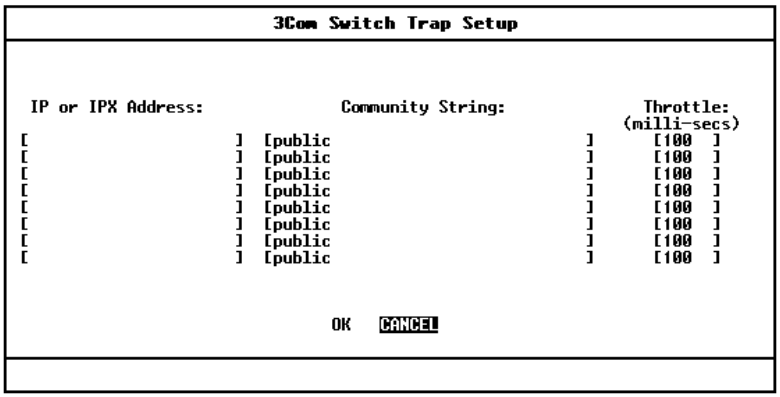


Figure 3-9 Trap Setup screen

The screen shows the following:

IP or IPX Address Type into this text field the IP or IPX address of the remote network management station to which traps should be sent.

Community String The community string allows a very simple method of authentication between the Switch 1005 and the remote Network Manager. The text string can be of 32 characters or less. If you want a Network Manager to receive traps generated by the device, you must enter the community string of the remote Network Manager into the trap table. The default community string is *public*.

Throttle To prevent a remote Network Manager receiving too many traps at once, you can configure the Switch 1005 to transmit traps with a delay between them. If several traps are generated at one time, they will be transmitted with the specified delay between them. The unit of throttle is one thousandth of a second. The default value is 100, which gives a minimum delay of one tenth of a second between each transmission.

Resetting the Switch 1005

If you suspect a problem with the Switch 1005, you can perform a reset.

1 From the Switch Main Menu, select the RESET option.

The Reset screen appears as shown in Figure 3-10.

2 Select OK.

Figure 3-10 Reset screen

CAUTION: *Resetting the Switch 1005 in this way is similar to performing a power off/on cycle. No setup information is lost. Performing a reset however, may cause some of the data being transmitted at that moment to be lost and statistic counters will be reset to zero.*

Initializing the Switch 1005

This screen allows you to perform a reset as described in the previous section, and in addition, returns non-volatile data stored on the unit to its factory defaults. Note that the IP address is not cleared. You should only initialize the Switch 1005 if:

- The configuration of the device no longer suits your network.
- Other efforts to solve problems have not succeeded.

To initialize the Switch:

1 From the Main Menu, select the INITIALIZE option.

The Initialization screen appears as shown in Figure 3-11.

2 Select OK.

Figure 3-11 Initialization screen

CAUTION: *Use Initialize with great care. The Switch 1005 configuration is cleared from memory and cannot be recovered. After initialization, all user information is lost and only default users are available. All ports are set to their default values, and are therefore enabled and available to all users. When initializing the Switch, take particular note of the following:*

- *Network loops will occur if you have set up resilient links. Before initializing the Switch, ensure you have disconnected the cabling for all your standby links.*

- *Network loops may occur if you are not careful when configuring your backplane connections. See "Advice for Setting Backplane Connections and Avoiding Loops" on page 2-4.*
- *Ports which form part of a VLT will fail and you will not be able to manage the Switch if your management station communicates via the VLT. To avoid this:*
  - **a** *Remove the VLT configuration from both ends of the VLT link before you initialize the Switch. Note that the port furthest from your management station should have its VLT configuration removed first.*
  - **b** *Reconfigure the VLT once the initialization is complete.*

Upgrading Software

When 3Com issues a new version of the software image for the Switch 1005, you can obtain it from the 3Com Bulletin Board Service, see Appendix C.

You use the Software Upgrade screen to download new software images. The protocol used for downloading software images is TFTP running over UDP/IP or IPX and will only work over the network, not via the serial port.

If a software download over IPX fails, you should enter the MAC address and port ID of your server into the switch database via the Database View screen and then attempt the download again.

1 From the Main Menu, select the SOFTWARE UPGRADE option.

The Software Upgrade screen is displayed as shown in Figure 3-12.

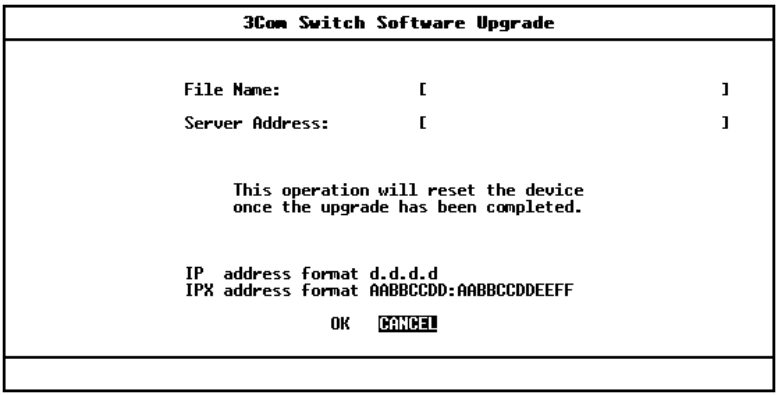


Figure 3-12 Software Upgrade screen

2 In the *File Name* field, type the name of the file that contains the software image to be downloaded to the Switch 1005. You must place the image file where it is accessible to the TFTP load request. Check with your system administrator if you are unsure of where to place the image file.

3 In the *Server Address* field, type the IP or IPX address of the host containing the software image to load.

4 Select OK.

During the download, the MGMT LED flashes green (fast flash, 1Hz) and the screen is locked. When the download is complete, the module is reset.

4 ADVANCED MANAGEMENT

Virtual LANs (VLANs)

Setting up Virtual Local Area Networks (VLANs) on the MSH Switch 1005 provides you with less time-consuming network administration and more efficient network operation.

The following sections explain more about the concept of VLANs and explain how they can be implemented on the Switch 1005.

What are VLANs?

A VLAN is defined as a group of location- and topology- independent devices that communicate as if they are on the same physical LAN. This means that LAN segments are not restricted by the hardware which physically connects them; the segments are defined by flexible user groups that you create using software.

With VLANs, you can define your network according to:

- **Organizational groups** — for example, you can have one VLAN for the Marketing department and one for the Finance department. Alternatively, you can have one VLAN for users with managerial status and one for users of director status.
- **Application groups** — for example, you can have one VLAN for users of email, and another VLAN for users of multimedia.

Benefits of VLANs

Implementing VLANs on your network has three main advantages:

- **It eases the change and movement of devices on IP networks**

  With traditional IP networks, network administrators spend much of their time dealing with moves and changes. If users move to a different IP subnet, the IP addresses of each workstation must be updated manually.

  With a VLAN setup, if a workstation on VLAN 1 is moved to a port in another part of the network, the network administrator only needs to configure the new port to belong to VLAN 1.

- **It helps to control broadcast traffic**

  With traditional networks, congestion can be caused by broadcast traffic which is directed to all network devices whether they require it or not. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices which need to communicate with each other.

- **It provides extra security**

  Devices within each VLAN can only communicate with devices in the same VLAN. If a device in VLAN 1 needs to communicate with devices in VLAN 2, the traffic must cross a router.

An Example

Figure 4-1 shows a network configured with port-based VLANs, where a VLAN consists of a set of switch ports. There are three VLANs — one for each of the departments who access the network. The membership of VLAN 1 is restricted to ports 1, 2, 3, 4 and 5 of Switch A; membership of VLAN 2 is restricted to ports 4, 5, 6, 7 and 8 of Switch B while VLAN 3 spans both Switches containing ports 6, 7, 8 of Switch A and 1, 2, 3 of Switch B.

In this simple example, each of these VLANs can be seen as a 'broadcast domain' — physical LAN segments that are not constrained by their physical location.

Specific configurations using the Switch are shown later in this chapter.

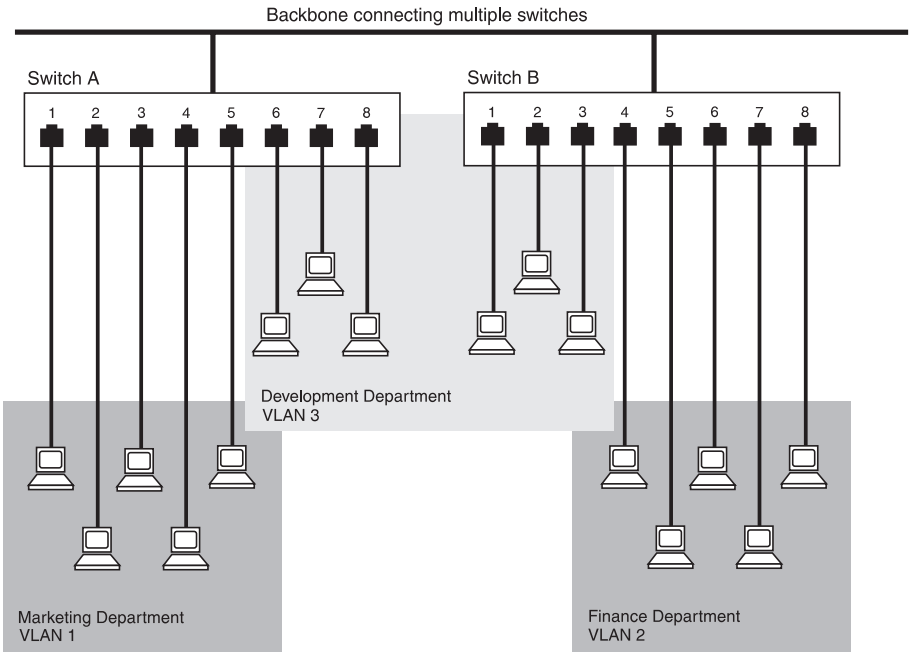


Figure 4-1 The concept of VLANs

VLANs and the Switch 1005

The Switch 1005 supports port-based VLANs, where a VLAN consists of a set of switch ports. Each switch port can only belong to one VLAN at a time, regardless of the device to which it is attached.

Each Switch 1005 can support up to 16 VLANs. However, you can have more than 16 VLANs in your entire network by connecting the 16 Switch VLANs to other VLANs using a router.

The Default VLAN

In any network setup, VLAN 1 is the Default VLAN. The Default VLAN is the only VLAN which allows an SNMP Network Manager to access the management agent of the unit. On a new Switch, all the ports belong to VLAN 1. If the devices attached to a port should belong to another VLAN, you need to use the VLAN Setup screen to place the port in that VLAN. For more information about the VLAN Setup screen, see "Setting Up VLANs on the Switch" on page 4-12.

Connecting VLANs to a Router

If the devices in a VLAN need to talk to devices in a different VLAN, each VLAN requires a connection to a router. Communication between VLANs can only take place if they are all connected to the router. A VLAN not connected to a router is isolated.

In the Switch 1005, VLANs are typically connected to routers using *backbone ports*. Backbone ports have the following attributes:

- Addresses received on backbone ports are not stored in the Switch Database.
- Frames with unknown addresses are forwarded to the backbone ports.

If you connect a Switch 1005 to a router using backbone ports, you need to specify one backbone port for each VLAN connected to the router.

Connecting Common VLANs Between Switches

In the Switch 1005, VLANs are typically connected to other Switch 1005 modules, SuperStack II Switch 1000 units and SuperStack II Switch 3000 units using backbone ports. Similar to the router connections, you normally require one backbone port per VLAN. However, to make the Switch-to-Switch connections more cost-effective, the Switch 1005 allows you to specify that one backbone port forms part of a Virtual LAN Trunk (VLT). A VLT is a connection which carries traffic for multiple VLANs between Switch modules and units. If you configure both ends of a Switch-to-Switch connection as part of a VLT, you only need that one connection for all the VLANs.

VLTs can only be used for links between Switch 1005 modules, SuperStack II Switch 1000 units and SuperStack II Switch 3000 units. You cannot use VLTs for Switch-router links.

If you specify that a backbone port on one VLAN is part of a VLT, that backbone port will become a backbone port for all the VLANs on the Switch — even if they had no backbone port before. If you then disable the VLT function on that port, the port becomes the backbone port for the Default VLAN (VLAN 1) and all other VLANs lose their backbone ports.

Using Non-routable Protocols

If you are running non-routable protocols on your network (for example, DEC LAT or NET BIOS), devices within one VLAN will not be able to communicate with devices in a different VLAN.

Using Unique MAC Addresses

If you connect a server with multiple network adapters to the Switch, we recommend that you configure each network adapter with a unique MAC address.

VLAN Configurations

Example 1

The example shown in Figure 4-2 illustrates a simple VLAN configuration comprising a single Switch 1005 with a 10Base-T Transceiver Module. The ports are divided between two VLANs; VLAN 1 is able to talk to VLAN 2 using the backbone port connection between each VLAN and the router.

To set up this configuration:

1. Use the VT100 screens to:
   - **a** Place ports 1-6 in VLAN 1.
   - **b** Place ports 7-12 in VLAN 2.
2. Connect a port in VLAN 1 to the router.
3. Use the VT100 screens to specify that the VLAN 1 port connected to the router is a backbone port.
4. Repeat steps 2 and 3 for VLAN 2.

You can set up this configuration more easily using 3Com's Transcend Enterprise Manager applications.

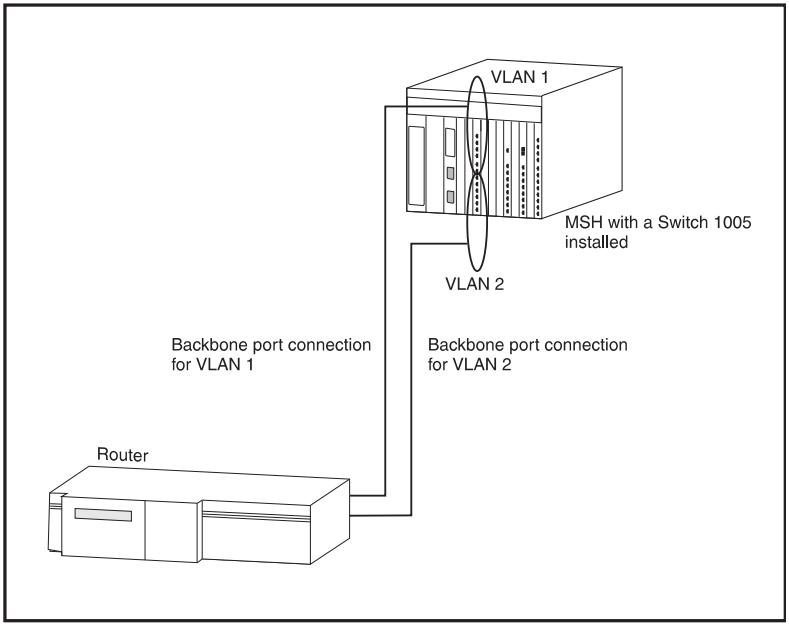


Figure 4-2 VLAN configuration with a single Switch 1005 module

Example 2

The example shown in Figure 4-3 illustrates two VLANs spanning two Switch 1005s, each with a Fast Ethernet Transceiver Module as port 1. VLAN 1 is able to talk to VLAN 2 using the backbone port connection between each VLAN and the router. Ports within the same VLAN which span the two Switches communicate using a VLT on the Fast Ethernet backplane.

To set up this configuration:

1. Use the VT100 screens to:
   - **a** Place ports 5-8 of both Switch 1005s in VLAN 1.
   - **b** Place ports 9-12 of both Switch 1005s in VLAN 2.
2. Connect port 1 of the right Switch 1005 to Server 1.
3. Connect port 1 of the left Switch 1005 to Server 2.
4. Use the VT100 screens to:
   - **a** Place port 1 of the right Switch 1005 in VLAN 2.
   - **b** Place port 1 of the left Switch 1005 in VLAN 1.
5. Connect port 28 on the right Switch 1005 to port 28 in the left Switch 1005.
6. Use the VT100 screens to specify that port 28 on the right Switch 1005 is a backbone port and part of a VLT.
7. Connect a VLAN 1 port on the left Switch 1005 to the router.
8. Use the VT100 screens to specify that the VLAN 1 port connected to the router is a backbone port.
9. Repeat steps 7 and 8 for VLAN 2.
10. Use the VT100 screens to specify that port 28 on the left Switch 1005 is part of a VLT.

You can set up this configuration more easily using 3Com's Transcend Enterprise Manager applications.

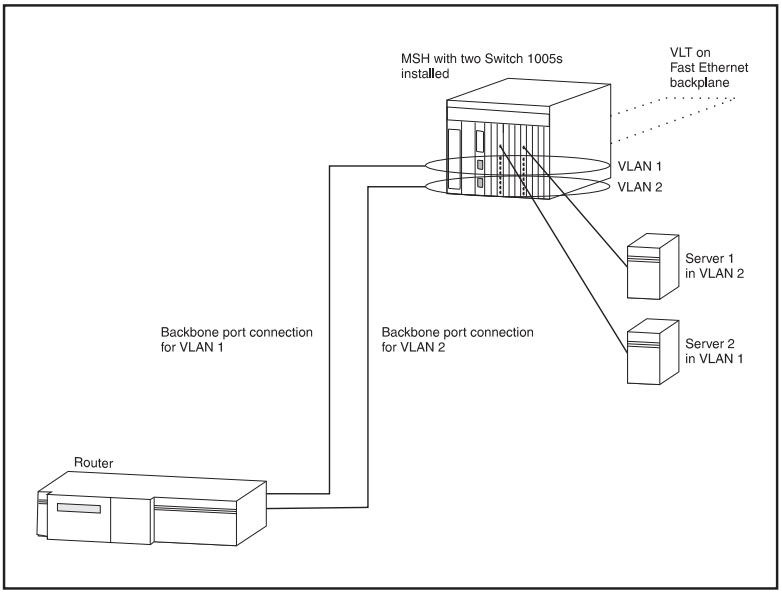


Figure 4-3 VLAN configuration with two Switch 1005s

Example 3

The example shown in Figure 4-4 illustrates two VLANs spanning three Switch 1005s (each with a 100FX Transceiver Module as port 1) and a basement SuperStack II Switch 3000 FX with a 100FX Downlink Module. Each Switch 1005 connects into the basement Switch 3000 FX using a VLT. The attached router allows the two VLANs to communicate with each other.

To set up this configuration:

1. Use the VT100 screens to:
   - **a** Place ports 5-8 of all the Switch 1005s in VLAN 1.
   - **b** Place ports 9-12 of all the Switch 1005s in VLAN 2.
2. Connect port 1 on each Switch 1005 to a port in the Switch 3000 FX.
3. Use the VT100 screens to:
   - **a** Specify that port 1 on each Switch 1005 is a backbone port.
   - **b** Specify that port 1 on each Switch 1005 is part of a VLT.
   - **c** Specify that each Switch 3000 FX port connected to a Switch 1005 is part of a VLT.
4. Connect port 1 of the Switch 3000 FX to Server 1.
5. Connect port 2 of the Switch 3000 FX to Server 2.
6. Use the VT100 screens to:
   - **a** Place port 1 of the Switch 3000 FX in VLAN 1.
   - **b** Place port 2 of the Switch 3000 FX in VLAN 2.
7. Connect two spare ports on the Switch 3000 FX to the router.
8. Use the VT100 screens to specify that one Switch 3000 FX port connected to the router is placed in VLAN 1, and the other is placed in VLAN 2.

You can set up this configuration more easily using 3Com's Transcend Enterprise Manager applications.

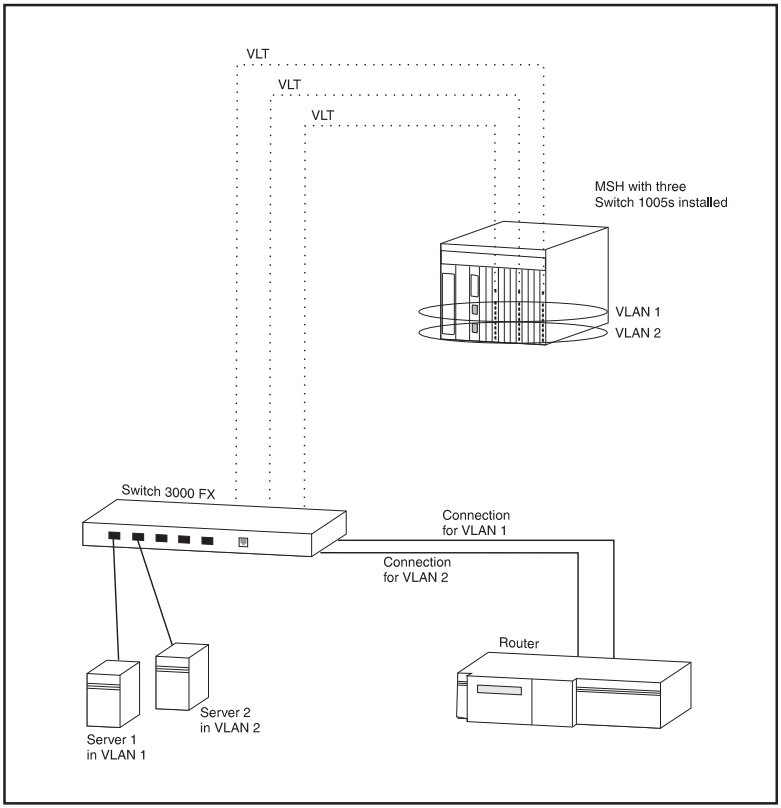


Figure 4-4 VLAN configuration with a Switch 3000 FX as a basement switch

Setting Up VLANs on the Switch

The VLAN Setup screen allows you to set up and manage VLANs on the Switch. To access the VLAN Setup screen:

1. From the VT100 Main Menu, select SWITCH MANAGEMENT. The Switch Management screen appears.
2. In the Management Level field, choose *VLAN*.
3. Choose the SETUP button. The VLAN Setup screen appears as shown in Figure 4-5.

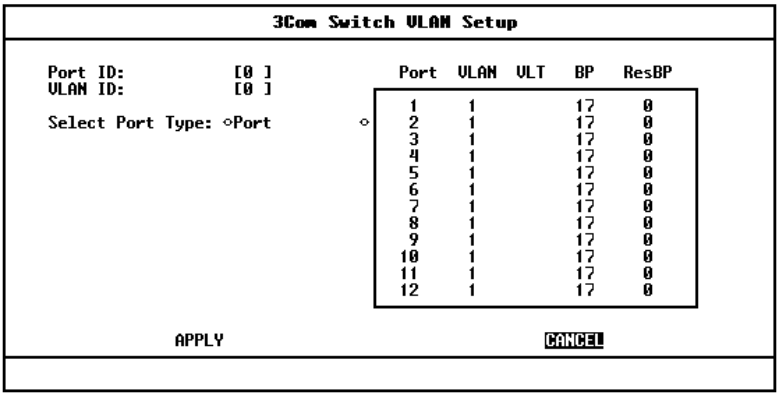


Figure 4-5 VLAN Setup screen

The screen shows the following:

Port ID *1,2,3 ... 26, 27, 28* This field allows you to enter the ID of the port that you want to set up.

VLAN ID *1,2,3 ... 14,15,16* This field allows you to enter the ID of the VLAN to which the specified port is to be assigned. By default, all ports belong to the Default VLAN (VLAN 1).

Select Port Type *Port/Backbone Port* This field allows you to specify whether the port specified in the Port ID field is a backbone port. A backbone port is used to connect each VLAN to the backbone of your network, and has the following attributes:

- Addresses received on the port are not stored in the Switch Database.
- Frames with unknown addresses received by the Switch are forwarded to the port.

Any port in a VLAN can be designated as the backbone port for that VLAN, but you can only have one backbone port per VLAN. By default, all ports belong to the Default VLAN (VLAN 1); because of this, an unconfigured Switch module can only have one backbone port.

If the Switch 1005 has a Fast Ethernet Transceiver Module installed, this automatically becomes the backbone port for the Default VLAN when you initialize the Switch. If the Switch has more than one Fast Ethernet Transceiver Module, the Transceiver Module with the lowest port number automatically becomes the backbone port for the Default VLAN. If the Switch has no Fast Ethernet Transceiver Module, but it uses port 28 to connect to the Fast Ethernet backplane, port 28 automatically becomes the backbone port for the Default VLAN.

A listbox containing the following fields:

Port The port ID for the entry.

VLAN The ID of the VLAN(s) that the port belongs to.

VLT Shows * if the port forms part of a Virtual LAN Trunk (VLT). A Virtual LAN Trunk is a connection which carries traffic for multiple VLANs between Switch units. For more information about VLTs in general, see "VLANs and the Switch 1005" on page 4-4. To specify that a port is a VLT, see "Port Setup" on page 3-7.

BP The backbone port for the VLAN specified in the VLAN field.

ResBP This field displays the resilient backbone port for the VLAN, if one exists. For more information about creating resilient links, see "Resilient Links" on page 3-17.

APPLY This button applies any changes to the VLAN database.

Assigning a Port to a VLAN

1. In the Port ID field, type the ID of the required port.
2. In the VLAN ID field, type the ID of the required VLAN.
3. Select APPLY.

CAUTION: *Initially, all Switch ports belong to the Default VLAN (VLAN 1). This VLAN is the only VLAN which allows an SNMP Network Manager to access the management agent of the unit. If you remove all ports from VLAN 1, then an SNMP Network Manager cannot manage the Switch.*

Specifying a Backbone Port

1. In the Port ID field, type the ID of the required port.
2. In the VLAN ID field, type the ID of the required VLAN.
3. In the Select Port Type field, select Backbone Port.
4. Select APPLY.

Specifying that a Backbone Port is Part of a VLT

1. From the BP field, note the ID of the backbone port. Refer to "Port Setup" in Chapter 3.

5 Status Monitoring and Statistics

This chapter describes how to view the current operating status of the Switch 1005 and how to carry out a remote poll to check the response of another network device. It also describes the Statistics screens for the Switch 1005, and advises you on actions to take if you see unexpected values for the statistics. Please note however, that as all networks are different, any actions listed are only suggestions.

Viewing statistics on a regular basis allows you to see how well your network is performing. If you keep simple daily records, you will see trends emerging and notice problems arising before they cause major network faults. Statistics can also help you get the best out of your network.

Summary Statistics

With the Switch Management screen displayed, choose to view statistics for the Switch 1005 *module*, then select the STATISTICS button.

A typical Switch Summary Statistics screen is displayed as shown in Figure 5-1.

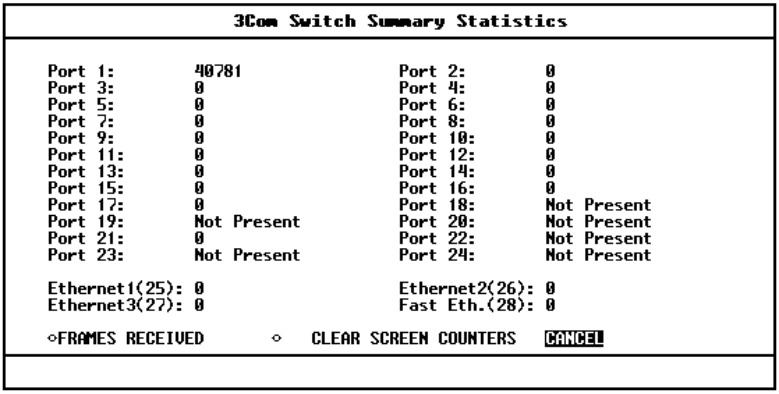


Figure 5-1 Switch Summary Statistics screen

The screen lists values for the current counter against every port on the Switch 1005 and it is refreshed approximately every two seconds. Once values have reached approximately 4.2 billion, they are reset to zero.

To view values for a particular counter, select the first button displayed at the foot of the Summary Statistics screen. Pressing the Space bar toggles through the available counters and as soon as you move away from the button, the screen is refreshed to show values for that counter.

FRAMES RECEIVED Displays the total number of frames that have been received by each port, including fragments and frames with errors.

FRAMES TRANSMITTED Displays the total number of frames that have been successfully transmitted by each port.

FRAMES FORWARDED Displays the total number of frames that were received by each port and forwarded to other ports.

FRAMES FILTERED Displays the total number of frames that were filtered because the destination station was on the same segment (port) as the source station.

MULTI/BROADCAST (RX) Displays the total number of frames received by each port that are addressed to a multicast or broadcast address.

MULTI/BROADCASTS (TX) Displays the total number of frames transmitted by each port that are addressed to a multicast or broadcast address.

ERRORS Displays the total number of errors that have occurred on each port. See the field description for Errors on page 5-7.

CLEAR SCREEN COUNTERS Use this button to set all counters shown on the screen to zero. Use this button for analysis if you wish to see changes in counters over a short period of time. This button does not clear the counters on the device. To zero actual device counters, you need to reset the Switch 1005, refer to "Resetting the Switch 1005" in Chapter 3.

Port Statistics

With the Switch Management screen displayed, choose to view statistics for a Switch 1005 *port*, then select the STATISTICS button.

A typical Switch Port Statistics screen is displayed as shown in Figure 5-2.

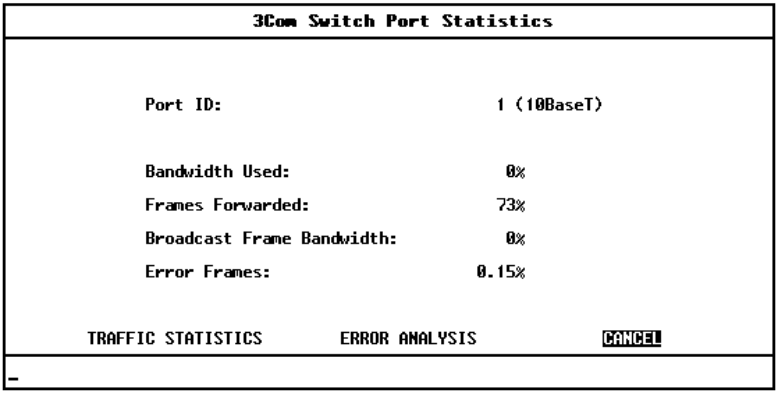


Figure 5-2 Switch Port Statistics screen

As well as showing statistics for the port, this screen allows you access to traffic and error counter screens.

The Port Statistics screen shows the following:

Port ID The ID of the port you are currently managing.

Bandwidth Used This counter provides a running average of the occupied bandwidth and is expressed as a percentage of the theoretical maximum bandwidth available. A sampling period of 1 minute is used. The value gives an indication of the general traffic level of the network. A high utilization for single station segments is an indication that your network is operating efficiently. However, if multiple end-stations are connected to this port and you see values of around 40% you should reconsider the topology of your network because each user will see degraded network performance.

Frames Forwarded This counter provides a running average of the proportion of the received frames that are forwarded and is expressed as a percentage of all received frames. A sampling period of 1 minute is used.

Broadcast Frame Bandwidth This counter provides a running average of the Broadcast frame bandwidth in use and is expressed as a percentage of a theoretical maximum bandwidth. A sampling period of 5 seconds is used.

Error Frames This counter provides a running average of the number of errors per 10,000 frames received and is expressed as a percentage. See the field description for Errors on page 5-7.

TRAFFIC STATISTICS Select this button to access traffic counters for this port.

ERROR ANALYSIS Select this button to access error counters for this port.

Port Traffic Statistics

With the Port Statistics screen displayed, select the TRAFFIC STATISTICS button.

A typical Port Traffic Statistics screen is displayed as shown in Figure 5-3.

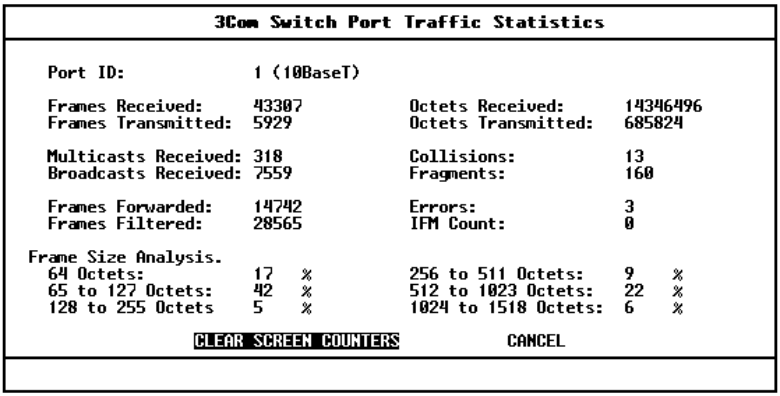


Figure 5-3 Port Traffic Statistics screen

The screen shows the following:

Port ID The ID of the port you are currently managing.

Frames Received The number of valid frames received by the port, including fragments and frames with errors.

Frames Transmitted The number of frames that have been successfully transmitted by the port.

Octets Received The number of octets received by the port. The calculation includes the MAC header and Cyclical Redundancy Check (CRC), but excludes preamble/Start-of-Frame-Delimiter (SFD). Octet counters are accurate to the nearest 256 octet boundary.

Octets Transmitted The number of octets transmitted by the port. The calculation includes the MAC header and CRC, but excludes preamble/SFD. Octet counters are accurate to the nearest 256 octet boundary.

Multicasts Received The number of frames successfully received that have a multicast destination address. This does not include frames directed to a broadcast address or frames received with errors.

Broadcasts Received The number of frames received that have a broadcast destination address. This does not include frames with errors.

Collisions An estimate of the total number of collisions that occurred when transmitting from the unit. Collisions are a normal part of Ethernet operation that occur when two devices attempt to transmit at the same time. A sudden sustained increase in the number of collisions may indicate a problem with a device or cabling on the network, particularly if this is not accompanied by an increase in general network traffic.

Fragments The total number of packets received that were not an integral number of octets in length or that had a bad Frame Check Sequence (FCS), and were less than 64 octets in length (excluding framing bits but including FCS octets).

Frames Forwarded The total number of frames which were received by the port and forwarded to their destination address.

Frames Filtered The total number of frames that were filtered because the destination address was on the same segment (port) as the source station.

Errors The total number of errors which have occurred on the port. Errors can be one of the following:

- CRC Alignment Errors
- Short Events
- Long Frames
- Late Events
- Jabbers

The value shown should be a very small proportion of the total data traffic.

IFM Count The total number of times Intelligent Flow Management (IFM) has had to operate to minimize packet loss.

Frame Size Analysis The number of frames of a specified length as a percentage of the total number of frames of between 64 and 1518 octets. This indicates the composition of frames on the network. The frame size ranges are:

- 64 octets
- 65 to 127 octets
- 128 to 255 octets
- 256 to 511 octets
- 512 to 1023 octets
- 1024 to 1518 octets

The composition of frames on your network may help you to analyze the efficiency of your network layer protocol.

CLEAR SCREEN COUNTERS Select this button to set all counters shown on the screen to zero. It is useful for trend analysis if you wish to see changes in counters over a short period of time. This button does not clear the counters on the device or affect counters at the network management station.

Port Error Analysis

With the Port Statistics screen displayed, select the ERROR ANALYSIS button.

A typical Port Error Analysis screen is displayed as shown in Figure 5-4.

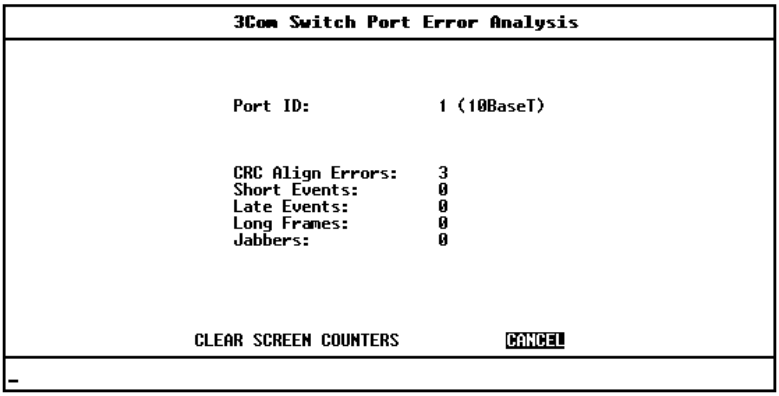


Figure 5-4 Port Error Analysis screen

The screen shows the following:

Port ID The ID of the port you are currently managing.

CRC Align Errors This counter is incremented by one for each frame with an CRC error or an alignment error. A CRC occurs if a frame of legal length has an invalid CRC and does not have a framing error. An alignment error occurs if a frame has a CRC error and does not contain an integral number of octets.

Alignment errors may be caused by a fault at the transmitting device. Change the transceiver or adapter card of the device connected to the port at the source of the problem. If this does not solve the problem, check cables and connections for damage.

Short Events This counter is incremented by one for each carrier event whose duration is less than the short event maximum time. Short events are error frames smaller than the minimum size defined for 802.3 frames. They may indicate externally generated noise causing problems on the network. Check the cabling routing and re-route any cabling which may be affected by external noise sources.

Late Events This counter is incremented by one each time a collision occurs after the valid packet minimum time. A late event is an out-of-window collision that may occur if your 802.3 LAN exceeds the maximum size as defined in the IEEE standard. A late event is also counted as a collision.

Long Frames This counter is incremented by one each time a frame is received whose octet count is greater than the maximum frame size but less than Jabber frame size. Long Frames are frames that exceed the maximum size defined for 802.3 frames (1518 octets). If you see a high number of long frames on your network, you should isolate the source of these frames and examine the transceiver or adapter card at the device. Some protocols may generate these frames.

Jabbers The total number of packets received that were longer than 8K octets (excluding framing bits, but including FCS octets).

CLEAR SCREEN COUNTERS Select this button to set all counters shown on the screen to zero. It is useful for trend analysis if you wish to see changes in counters over a short period of time. This button does not clear the counters on the device or affect counters at the network management station.

Status Monitoring

The status screen provides read-only information about the Switch 1005. To access the screen, from the Main Menu, select the STATUS option.

The Status screen is displayed as shown in Figure 5-5.

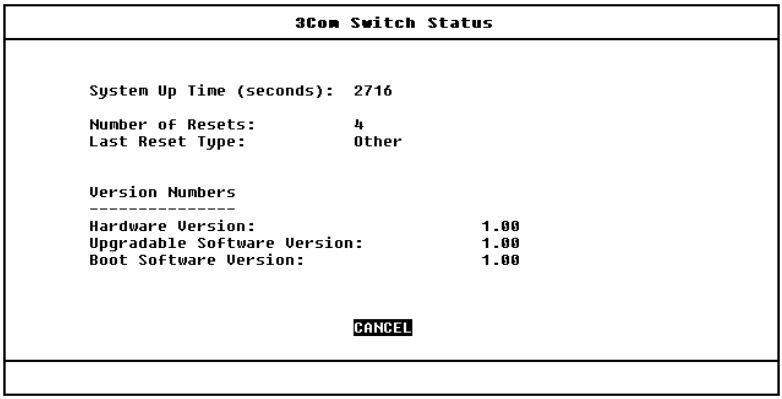


Figure 5-5 Status screen

The screen shows the following:

System Up Time (seconds) The number of seconds this unit has been running since the last reset or power off/on cycle.

Number Of Resets The total number of system resets since the Switch 1005 was first installed or initialized; either power-on, manual reset or a watchdog expiry. If you have a problem, this information may be useful for your technical support representative.

Last Reset Type *other/command/watchdog/power- reset/system-error* This field indicates the cause of the last reset. It may be due to management command, watchdog timeout expiry, power interruption, a manual reset or a system error. If you have a problem, this information may be useful for your technical support representative.

Hardware Version The hardware version number of the Switch 1005. You should note this number in case you need to quote it to your technical support representative.

Upgradable Software Version The version number of the software image stored in Flash EPROM. This version number is automatically updated when you download new software. You should note this number in case you need to quote it to your technical support representative.

Boot Software Version This is the version number of the Boot software stored on the Switch 1005. You should note this number in case you need to quote it to your technical support representative.

Remote Polling

The Remote Poll screen allows you to send a single frame to a remote device to see if that device is responding. This can help to locate the source of a network problem. It is also particulary helpful in locating devices that support IP, IPX and ping but are not manageable by SNMP.

1 To access the Remote Poll screen, from the Main Menu, select Remote Poll. The screen is displayed as shown in Figure 5-6.

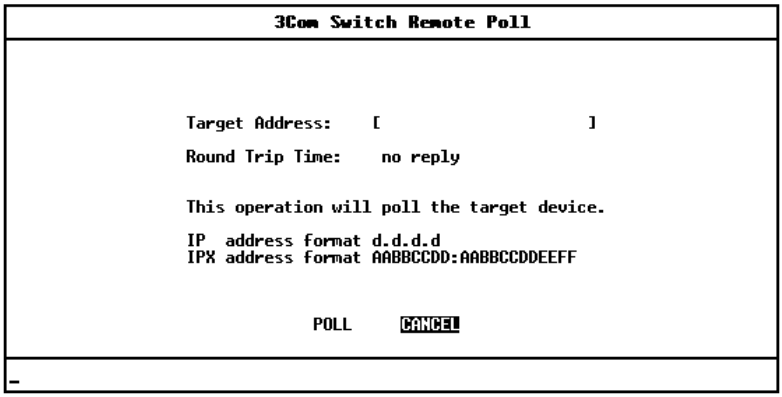


Figure 5-6 Remote Poll screen

2 In the *Target Address* field, type in the IP or IPX address of the device you want to poll.

3 Select the POLL button at the foot of the screen.

When the poll is complete, the *Round Trip Time* field shows the interval in milliseconds between sending the frame to the target device and receiving a response at the Switch 1005. If the target device does not respond after approximately 10 seconds, this field will display *no reply*.

You can use an SNMP Network Manager to configure the Switch to send regular IP or IPX ping packets to a maximum of ten other network devices. If a device fails to respond to four consecutive ping requests, a trap is sent by the Switch to the management station.

6 PROBLEM SOLVING

Spot Checks

This chapter explains how to check for problems and solve them. It is good practice to carry out regular checks of your MSH equipment and it could allow you spot a potential problem before it occurs.

Check the following:

- **LEDs** — Press the Lamp Test button located on the MSH display panel. All yellow LEDs should light continuously and all bi-color LEDs should flash their two colors alternately.
- **Cabling** — Check that all external cabling connections are secure and that no cables are pulled taut.
- **Modules** — Check that all modules are secured in position and that their ejectors are locked. All modules should be flush in the chassis with each other.

  If individual LEDs do not respond to the Lamp Test, the LEDs are faulty. If, however, all LEDs on a single module fail to light, and all other checks are satisfactory, there is a fault with the module or the MSH chassis. Refer to "Identifying Fault Conditions with the LEDs" later in this chapter.

Identifying Fault Conditions with the LEDs

The following table shows how you can identify possible fault conditions that may occur during normal operation. It also describes actions that may resolve the problem:

LED	Color	Indicates	Try the following actions
PWR (Power)	Off	Power is not reaching the module	■ Check that the Power LED on the MSH chassis is not lit red. If it is, refer to your chassis user documentation. ■ Ensure the MSH chassis is powered-up correctly with all power leads securely connected. ■ Ensure the module is fully engaged into the chassis. ■ Contact your supplier for advice.
		Faulty LED	■ Test LEDs to confirm.
	Amber	Fault occurred on this module during POST or normal operation	
BACKPLANE E, FE	Off	Fault	■ Ensure module is fully engaged into chassis and the backplane connectors are fully mated.
		Faulty LED	■ Test LEDs to confirm.
1 - 12 (External port status)	Off	Fault	■ Check all connections are secure. ■ Check all cables and connectors for signs of damage.

If you cannot solve the problem, contact your local supplier, or proceed as described in Appendix C.

VT100 Problems

The SNMP Network Manager cannot access the device:

Check the device's IP address, subnet mask and default router are correctly configured, and that the device has been reset. Check that the device's IP address is correctly recorded by the SNMP Network Manager (refer to the user manual for the Network Manager).

The Telnet workstation cannot access the device:

Check that your terminal or terminal emulator is correctly configured to operate as a VT100 terminal.

Check the device's IP address, subnet mask and default router are correctly configured, and that the device has been reset. Ensure that you enter the IP address correctly when invoking the Telnet facility.

Traps are not received by the SNMP Network Manager:

Check the SNMP Network Manager's IP address and that the community string is correctly configured.

The SNMP Network Manager or Telnet workstation can no longer access the device:

Check that Remote Telnet access or Community-SNMP access is enabled.

Check that the port through which you are trying to access the device has not been disabled, see "Port Setup" in Chapter 3. If it is enabled, check the connections and network cabling at the port.

Check that the port though which you are trying to access the device is still in VLAN 1 (the Default VLAN). See "Setting Up VLANs on the Switch" in Chapter 4.

Try accessing the device through a different port. If you can now access the device, a problem with the original port is indicated. Re-examine the connections and cabling.

Possibly there is a network problem preventing you accessing the device over the network. Try accessing the device through the serial port.

You forget your password and cannot log in:

If you are not one of the default users (monitor, manager or security), another user having 'security' access level can log in, delete your user name, and create a new user name for you, with a new password.

Alternatively, another user having 'security' access level can log in and initialize the device. This will return all configuration information, including passwords, to the initial values.

In the case where no-one knows a password for a security level user, contact your supplier.

Switch 1005 Operation Problems

You see network problems and the Packet LED is on continuously with constant collisions (viewed using the Port Traffic Statistics screen, see "Port Traffic Statistics" in Chapter 5).

You are using PACE equipped devices and have PACE enabled at both ends of the link. PACE must only be enabled at one end of the Switch-device link. Disable PACE on the Switch port as described in "Port Setup" in Chapter 3.

Changing links LK1 to LK5 has no effect on external port configuration.

Link settings and internal port settings are not synchronized. Link settings can be overridden by management and these overrides are retained through power off/on cycles. It may be that internal ports were configured for a different Switch 1005 previously installed into this slot.

You cannot see internal backplane connection E3 (port 27) on any screen.

Backplane connection E3 (port 27) disappears from all screens if there is an expansion module fitted to your Switch 1005 and you have four 4 Port 10BASE-T Transceiver Modules installed. Port 27 will reappear and will be fully manageable if you remove one 4 Port 10BASE-T Transceiver Module.

You have added the Switch 1005 to an already busy network, and response times and traffic levels have increased.

You may have added a group of users to one of the Switch 1005 ports via a repeater or switch, and not turned off IFM. Turn off IFM on any port that is connected to multiple devices. See "Port Setup" in Chapter 3.

You have a chassis with a Management Module and at least one Switch 1005 module installed, and you have just installed another Switch module. One or more of the backplane LEDs are continuously lit.

You have installed the latest Switch 1005 into the chassis when the chassis and the Management Module were powered off, and due to the way the Management Module behaves when it is powered on (see "Operation after Power-up" in Chapter 2), this has caused a network loop on the chassis backplane. With the chassis and Management Module powered on, remove the latest Switch 1005 and insert it into another slot. If there are no spare slots, insert a module of a different type into the slot vacated by the Switch module for 30 seconds, and then replace that module with the Switch module.

You have more than one Switch 1005 in your chassis. The network does not appear to pass traffic, and one or more of the backplane LEDs are continuously lit.

You may have caused a network loop on the chassis backplane. See "Advice for Setting Backplane Connections and Avoiding Loops" in Chapter 2.

A SCREEN ACCESS RIGHTS

The following table lists the rights assigned to each level of user for accessing and editing Switch 1005 screens via the VT100 interface.

The access rights granted to Monitor level are all read-only. All other access rights are read-and-write.

Screen	Available to...
Logon	Monitor
	Manager
	Security
Main Menu	Monitor
	Manager
	Security
Switch Management	Monitor
	Manager
	Security
Port Statistics	Monitor
	Manager
	Security
Port Statistics (Traffic)	Monitor
	Manager
	Security
Port Statistics (Errors)	Monitor
	Manager
	Security

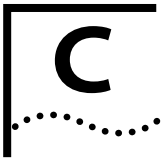
Screen	Available to...
Unit Statistics	Monitor
	Manager
	Security
Switch Database View	Monitor
	Manager
	Security
Unit Setup	Monitor
	Manager
	Security
Port Setup	Monitor
	Manager
	Security
Unit Resilience	Monitor
	Manager
	Security
Port Resilience	Monitor
	Manager
	Security
Remote Poll	Manager
	Security
Security Menu	Monitor
	Manager
	Security
Create User	Security
Delete User	Security
Local Security	Security
Change User	Monitor
	Manager
	Security

Screen	Available to...
Status	Monitor
	Manager
	Security
Setup	Monitor
	Manager
	Security
Trap Setup	Monitor
	Manager
	Security
Software Upgrade	Security
Initialize	Security
Reset	Manager
	Security

B TECHNICAL SPECIFICATION

Physical Dimensions	Height: 283mm (11.1 inches) x Width: 25mm (1 inch) x Depth 312mm (12.3 inches) Weight: 560g (1.2lbs)
Environmental Requirements	
Operating Temperature	0° to 50° C (32° to 122°F)
Operating Humidity	10 to 95% relative humidity, non-condensing
Standards	EN60068 (IEC68)
Safety	
Agency Certifications	UL 1950, EN60950, CSA 22.2 No. 950, ECMA 97
Electromagnetic Emissions (Agency Certification)	*Note that to comply with these standards, shielded cables must be used.* EN55022 Class B, FCC Part 15 Class A, C108.8-M1983 Class A, EN 50082-1 (IEC801 Parts 2-5)
Heat Dissipation	24 watts maximum

Standards Supported	**SNMP** ■ SNMP protocol (RFC 1157) ■ MIB-II (RFC 1213) ■ Bridge MIB (RFC 1286) ■ Repeater MIB (RFC 1516) ■ VLAN MIB (RFC 1573) ■ RMON MIB (RFC 1271) ■ BOOTP (RFC 951)	**Terminal Emulation** ■ Telnet (RFC 854) **Protocols Used for Administration** ■ UDP (RFC 768) ■ IP (RFC 791) ■ ICMP (RFC 792) ■ TCP (RFC 793) ■ ARP (RFC 826) ■ TFTP (RFC 783)



TECHNICAL SUPPORT

3Com provides easy access to technical support information through the variety of services described in this appendix.

Online Technical Services

3Com offers worldwide product support seven days a week, 24 hours a day, through the following online systems:

- 3Com Bulletin Board Service (3ComBBS)
- World Wide Web site
- 3ComForum on CompuServe®
- 3ComFacts℠ automated fax service

3Com Bulletin Board Service

3ComBBS contains patches, software, and drivers for all 3Com products, as well as technical articles. This service is available via modem or ISDN seven days a week, 24 hours a day.

Access by Modem

To reach the service by modem, set your modem to 8 data bits, no parity, and 1 stop bit.

Call the telephone number nearest you:

Country	Data Rate	Telephone Number
Australia	up to 14400 bps	(61) (2) 9955 2073
France	up to 14400 bps	(33) (1) 69 86 69 54
Germany	up to 9600 bps	(49) (89) 627 32 188 **or** (49) (89) 627 32 189
Hong Kong	up to 14400 bps	(852) 2537 5608
Italy (fee required)	up to 14400 bps	(39) (2) 273 00680
Japan	up to 14400 bps	(81) (3) 3345 7266
Singapore	up to 14400 bps	(65) 534 5693
Taiwan	up to 14400 bps	(886) (2) 377 5838
U.K.	up to 28800 bps	(44) (1442) 278278
U.S.	up to 28800 bps	(1) (408) 980 8204

Access by ISDN

ISDN users can dial-in to 3ComBBS using a digital modem for fast access up to 56 Kbps. To access 3ComBBS using ISDN, dial the following number:

(408) 654 2703

World Wide Web Site

Access the latest networking information on 3Com's World Wide Web site by entering our URL into your Internet browser:

`http://www.3Com.com/`

This service features news and information about 3Com products, customer service and support, 3Com's latest news releases, selected articles from 3TECH™ (3Com's award-winning technical journal) and more.

3ComForum on CompuServe

3ComForum is a CompuServe-based service containing patches, software, drivers, and technical articles about all 3Com products, as well as a messaging section for peer support. To use 3ComForum, you need a CompuServe account.

To use 3ComForum:

1. Log on to CompuServe.
2. Enter **`go threecom`** .
3. Press [Return] to see the 3ComForum main menu.

3ComFacts Automated Fax Service

3Com Corporation's interactive fax service, 3ComFacts, provides data sheets, technical articles, diagrams, and troubleshooting instructions on 3Com products 24 hours a day, seven days a week.

Call 3ComFacts using your touch-tone telephone. International access numbers are:

Country	Telephone Number
Hong Kong	(852) 2537 5610
U.K.	(44) (1442) 278279
U.S.	(1) (408) 727 7021

Local numbers are available within the following countries:

Country	Telephone Number
Australia	800 123853
Belgium	0800 71279
Denmark	800 17319
Finland	98 001 4444
France	05 90 81 58
Germany	0130 8180 63
Italy	1678 99085

Country	Telephone Number
Netherlands	06 0228049
Norway	800 11062
Portugal	0505 442607
Russia (Moscow only)	956 0815
Spain	900 964445
Sweden	020 792954
U.K.	0800 626403

Support from Your Network Supplier

If additional assistance is required, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you contact your network supplier for assistance, have the following information ready:

- Diagnostic error messages
- A list of system hardware and software, including revision levels
- Details about recent configuration changes, if applicable

If you are unable to contact your network supplier, see the following section on how to contact 3Com.

Support from 3Com

If you are unable to receive support from your network supplier, technical support contracts are available from 3Com.

In the U.S. and Canada, call **(800) 876-3266** for customer service.

If you are outside the U.S. and Canada, contact your local 3Com sales office to find your authorized service provider:

Country	Telephone Number	Country	Telephone Number
Australia (Sydney)	(61) (2) 959 3020	Japan	(81) (3) 33457251
(Melbourne)	(61) (3) 653 9515	Mexico	(525) 531 0591
Belgium*	0800 71429	Netherlands*	06 0227788
Brazil	(55) (11) 546 0869	Norway*	800 13376
Canada	(416) 498 3266	Singapore	(65) 538 9368
Denmark*	800 17309	South Africa	(27) (11) 803 7404
Finland*	0800 113153	Spain*	900 983125
France*	05 917959	Sweden*	020 795482
Germany*	0130 821502	Taiwan	(886) (2) 577 4352
Hong Kong	(852) 868 9111	United Arab Emirates	(971) (4) 349049
Ireland*	1 800 553117	U.K.*	0800 966197
Italy*	1678 79489	U.S.	(1) (408) 492 1790

* These numbers are toll-free.

Returning Products for Repair

A product sent directly to 3Com for repair must first be assigned a Return Materials Authorization (RMA) number. A product sent to 3Com without an RMA number will be returned to the sender unopened, at the sender's expense.

To obtain an RMA number, call or fax:

Country	Telephone Number	Fax Number
U.S. and Canada	(800) 876 3266, option 2	(408) 764 7120
Europe	31 30 60 29900, option 5	(44) (1442) 275822
Outside Europe, U.S., and Canada	(1) (408) 492 1790	(1) (408) 764 7290

GLOSSARY

10BASE-T

The IEEE 802.3 specification for Ethernet over Unshielded Twisted Pair (UTP).

100BASE-FX

100Mbps Ethernet implementation over fiber.

100BASE-TX

100Mbps Ethernet implementation over Category 5 and Type 1 Twisted Pair cabling.

ageing

The automatic removal of dynamic entries from the Switch Database which have timed-out and are no longer valid.

backbone

The part of a network used as the primary path for transporting traffic between network segments.

backbone port

A port which does not learn device addresses, and which receives all frames with an unknown address. Backbone ports are normally used to connect the Switch to the backbone of your network.

backplane

The internal path between modules within the MSH chassis.

bandwidth

Information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10Mbps, the bandwidth of Fast Ethernet is 100Mbps.

baud rate

The switching speed of a line. Also known as *line speed*.

BOOTP

The BOOTP protocol allows you to automatically map an IP address to a given MAC address each time a device is started. In addition, the protocol can assign the subnet mask and default gateway to a device.

bridge

A device that interconnects local or remote networks no matter what higher level protocols are involved. Bridges form a single logical network, centralizing network administration.

broadcast

A message sent to all destination devices on the network.

broadcast storm

Multiple simultaneous broadcasts that typically absorb available network bandwidth and can cause network failure.

CSMA/CD

Channel access method used by Ethernet and IEEE 802.3 in which devices transmit only after finding the data channel clear for some period of time. When two devices transmit simultaneously, a collison occurs and the colliding devices delay their retransmissions for a random length of time.

data center switching

The point of aggregation within a corporate network where a switch provides high-performance access to server farms, a high-speed backbone connection and a control point for network management and security.

Ethernet

A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks operate at 10Mbps using CSMA/CD to run over cabling.

Fast Ethernet

100Mbps technology based on the Ethernet/CD network access method.

forwarding

The process of sending a frame toward its destination by an internetworking device.

full duplex

A system which allows frames to be transmitted and received simultaneously and, in effect, doubles the bandwidth available on a link.

IFM

Intelligent Flow Management. A means of holding packets back at the transmit port of the connected end-station. Prevents packet loss at a congested switch port.

IPX

Internetwork Packet Exchange. A protocol allowing communication in a NetWare network.

IP address

Internet Protocol address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with full-stops (periods), and is made up of a network section, an optional subnet section and a host section.

LAN

Local Area Network. A network of connected computing resources (such as PCs, printers, servers) covering a relatively small geographic area (usually not larger than a floor or building). Characterized by high data rates and low error rates.

latency

The delay between the time a device receives a frame and the time the frame is forwarded out of the destination port.

line speed

See *baud rate*.

main port

The port in a resilient link that carries data traffic in normal operating conditions.

MIB

Management Information Base. Stores a device's management characteristics and parameters. MIBs are used by the Simple Network Management Protocol (SNMP) to contain attributes of their managed systems. The Switch contains its own internal MIB.

multicast

Single packets copied to a specific subset of network addresses. These addresses are specified in the destination-address field of the packet.

PACE

Priority Access Control Enabled. 3Com's innovative technology which works in conjunction with a switch to control the latency and jitter associated with the transmission of multimedia traffic over Ethernet and Fast Ethernet.

protocol

A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.

resilient link

A pair of ports that can be configured so that one will take over data transmission should the other fail. See also *main port* and *standby port*.

RJ-45

Standard 8-wire connectors for IEEE 802.3 10BASE-T networks.

RMON

Remote Monitoring. Subset of SNMP MIB II allows monitoring and management capabilities by addressing up to ten different groups of information.

server farm

A cluster of servers in a centralized location serving a large user population.

SNMP

Simple Network Management Protocol. A protocol originally designed to be used in managing TCP/IP internets. SNMP is presently implemented on a wide range of computers and networking equipment and may be used to manage many aspects of network and end-station operation.

SmartAgent

Intelligent management agents in devices and logical connectivity systems that reduce the computational load on the network management station and reduce management-oriented traffic on the network.

standby port

The port in a resilient link that will take over data transmission if the main port in the link fails.

switch

A device which filters, forwards and floods frames based on the frame's destination address. The switch learns the addresses associated with each switch port and builds tables based on this information to be used for the switching decision.

TCP/IP

A layered set of communications protocols providing Telnet terminal emulation, FTP file transfer, and other services for communication among a wide range of computer equipment.

Telnet

A TCP/IP application protocol that provides virtual terminal service, letting a user log in to another computer system and access a host as if the user were connected directly to the host.

TFTP

Trivial File Transfer Protocol. Allows you to transfer files (such as software upgrades) from a remote device using your Switch's local management capabilities.

Transcend

3Com's network management system used to manage all of 3Com's networking solutions.

UDP

User Datagram Protocol. An Internet standard protocol that allows an application program on one device to send a datagram to an application program on another device.

VLAN

Virtual LAN. A group of location- and topology-independent devices that communicate as if they are on a common physical LAN.

VLT

Virtual LAN Trunk. A connection which carries traffic for multiple VLANs between Switch 1005 modules, SuperStack II Switch 1000 units and SuperStack II Switch 3000 units.

VT100

A type of terminal which uses ASCII characters. VT100 screens have a text-based appearance.

INDEX

N

O

P

R

S

T

U

V

W

Z

LIMITED WARRANTY

HARDWARE: 3Com warrants its hardware products to be free from defects in workmanship and materials, under normal use and service, for the following lengths of time from the date of purchase from 3Com or its Authorized Reseller:

Internetworking products	**One year**
Network adapters	**Lifetime**
Ethernet stackable hubs and unmanaged Ethernet fixed port repeaters	**Lifetime*** **(One year if not registered)**
***Power supply and fans in these stackable hubs and unmanaged repeaters**	**One year**
Other hardware products	**One year**
Spare parts and spares kits	**90 days**

If a product does not operate as warranted during the applicable warranty period, 3Com shall, at its option and expense, repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of 3Com. Replacement products may be new or reconditioned. Any replaced or repaired product or part has a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

3Com shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to 3Com pursuant to any warranty.

SOFTWARE: 3Com warrants that the software programs licensed from it will perform in substantial conformance to the program specifications therefor for a period of ninety (90) days from the date of purchase from 3Com or its Authorized Reseller. 3Com warrants the magnetic media containing software against failure during the warranty period. No updates are provided. 3Com's sole obligation hereunder shall be (at 3Com's discretion) to refund the purchase price paid by Customer for any defective software products, or to replace any defective media with software which substantially conforms to 3Com's applicable published specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials. 3Com makes no warranty that its software products will work in combination with any hardware or applications software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third party products listed in the 3Com software product documentation or specifications as being compatible, 3Com will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a “bug” or defect in the third party's product.

STANDARD WARRANTY SERVICE: Standard warranty service for hardware products may be obtained by delivering the defective product, accompanied by a copy of the dated proof of purchase, to 3Com's Corporate Service Center or to an Authorized 3Com Service Center during the applicable warranty period. Standard warranty service for software products may be obtained by telephoning 3Com's Corporate Service Center or an Authorized 3Com Service Center, within the warranty period. Products returned to 3Com's Corporate Service Center must be pre-authorized by 3Com with a Return Material Authorization (RMA) number marked on the outside of the package, and sent prepaid, insured, and packaged appropriately for safe shipment. The repaired or replaced item will be shipped to Customer, at 3Com's expense, not later than thirty (30) days after receipt by 3Com.

WARRANTIES EXCLUSIVE: IF A 3COM PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER’S SOLE REMEDY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM’S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. 3COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

3COM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE) SHALL 3COM BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS,EVEN IF 3COM OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Some states do not allow the exclusion of implied warranties or the limitation of incidental or consequential damages for consumer products, so the above limitations and exclusions may not apply to you. This warranty gives you specific legal rights which may vary from state to state.

GOVERNING LAW: This Limited Warranty shall be governed by the laws of the state of California.

3Com Corporation
5400 Bayfront Plaza
Santa Clara, CA 95052-8145
(408) 764-5000
1/1/94

ELECTROMAGNETIC COMPATIBILITY STATEMENTS

FCC Statement

This equipment has been tested with a class A computing device and has been found to comply with part 15 of FCC Rules. Operation in a residential area may cause unacceptable interference to radio and TV receptions requiring the operator to take whatever steps are necessary to correct the interference.

CSA Statement

This Class A digital apparatus meets all requirements of the Canadian Interference-causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Information To The User

If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna.
- Relocate the equipment with respect to the receiver.
- Move the equipment away from the receiver.
- Plug the equipment into a different outlet so that equipment and receiver are on different branch circuits.

If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions. The user may find the following booklet prepared by the Federal Communications Commission helpful:

How to Identify and Resolve Radio-TV Interference Problems

This booklet is available from the U.S. Government Printing Office, Washington, DC 20402, Stock No. 004-000-00345-4.

In order to meet FCC emissions limits, this equipment must be used only with cables which comply with IEEE 802.3.